VOLUME 27 NUMBER 13 | $5.00

NETWORKWORLD

THE CONNECTED ENTERPRISE ≡ JULY 12, 2010

THE SECURITY BLIND SPOT

THE DARK SIDE OF VIRTUALIZATION & CLOUD COMPUTING

IT'S WHAT YOU CAN'T SEE THAT SCARES YOU.

ndc

THE NEW DATA CENTER

STRATEGIES & TECHNOLOGIES FOR OPTIMIZING IT

NetworkWorld.com

WHAT'S *the* BUSINESS PROBLEM?

SCATTERED WORKFORCE

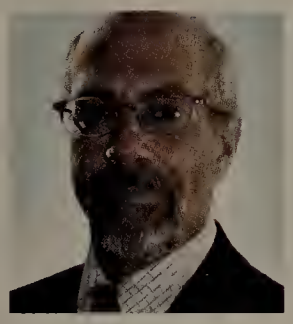
the QWEST SOLUTION: The more workers you have on the road, the greater the risk of hijacked data. Qwest's suite of security solutions can help make sure your critical information is accessible to those who need it, while protecting it from those who don't. So your business can safely stay on the go. **Solve more problems at qwestsolutions.com.**

Qwest BUSINESS

FROM THE EDITOR | JOHN DIX

The White House plan to safeguard cyberspace

The plan to "reduce cybersecurity vulnerabilities and improve online privacy protections" floated in June by Howard Schmidt, the Cybersecurity Coordinator and Special Assistant to the President, is comprehensive and an important step in the right direction.



To its credit, the administration released the National Strategy for Trusted Identities in Cyberspace (NSTIC) as a draft (tinyurl.com/24daffh, comments due by July19), realizing that something this big and complex needs input.

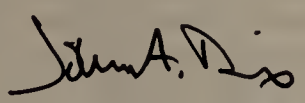
The basic idea is to ensure online commerce continues to flourish by using trusted digital identities and authentication to address core security issues. The government will be the "primary enabler, first adopter and key supporter" of what it calls an Identity Ecosystem, but consumers would be able to use the resultant tools to safeguard everything from online banking and shopping to accessing health records.

Instead of issuing its own "Internet license", the government wants identity service providers to come out with or make existing credentials interoperable so consumers have a choice when it comes to suppliers and can count on the fact that other merchants in the ecosystem will accept those credentials. Ideally, for example, I would be able to use my Bank of America SafePass card — which generates a number used as a second factor when I log onto the bank's sitė— to complete a transaction with a Web store.

As some have pointed out, there is little discussion in the proposal about how we would ensure the person applying for a credential is who they say they are. If you can game the system from the get-go that could be even more dangerous than the problems we face today. That said, use of existing credentials would help circumvent that concern. My bank knows who I am.

Others have taken issue with the idea of centralizing identities, saying that's putting all our eggs in one basket. Having multiple identities is inherently more secure, they argue. Perhaps, but that's what we have today and we still have these problems, so that argument doesn't seem to hold water. Then there is the whole big brother thing, the fear of the government logging our activities. Here again, the fact that this is government sanctioned vs. government issued, should help.

The point is that the proposal isn't fully baked, nor does it pretend to be. It will be interesting to see what comes out of this review period and see how the plan morphs. The authors also recognize that trusted digital identities address only one part of the layered security needed, but count us among those that think this is a good first step.



jdix@nww.com
Twitter.com/JDNWW

inside

JULY 12, 2010

peersay

Too soon to pin down the cloud

FIRST, WHY WOULD I care whether I get the entire stack from one provider, if I am looking for an open cloud platform, which I can extend or reconfigure using components from various providers? (Re: Only Microsoft and Red Hat have all the pieces to build clouds, Red Hat says; tinyurl.com/37b9s7r.)

Which brings me to "too early" — second issue: clouds are not yet standardized. There's no simple and easy way to migrate an app from EC2 to app engine. It's risky to invest into cloud apps right now. Give it some time, push for standardization, then, when standards-compliant service providers start operating large public clouds, carefully start deploying apps conforming to standards. Wait some more years until security issues are ironed out, and only then fully embrace the cloud paradigm.

Third, I'm not fully convinced that the cloud is the proper solution to all networked apps. There'll always be Photoshop or mathlab or other apps that are unreasonably run remotely. There'll always be apps manipulating data that is sensitive that you won't want it to travel over public networks, let alone be stored in a publicly available cloud. Therefore, I don't think the desktop or the dedicated server will die any time soon or not so soon.

Fourth, to downplay what SpringSource does (some very neat app servers, among other things, plus most components to set up a really programmer-friendly cloud), is stupid. The framework they created is an essential piece of work to make enterprise Web apps palatable. Working without spring core feels like wading through knee-deep mud. Programmer time is still one of the most expensive resources in the industry.

Anon

Cisco standard: Innovation or monopoly?

IF THE STANDARD only operates on Cisco gear then how is that a standard? Standards become useful only if most vendors support them. Sure, Cisco can develop whatever it wants and can do this to meet the needs of the customer base that it wants to sell to. (Re: Cisco wants to be the standard; tinyurl.com/34fc78b.)

If you are a bleeding-edge customer and you want or require the features and functions from a pre-standard offering, then you purchase it and live with the possibility that it may be proprietary and only operate with that vendor's gear. While it is true that Cisco has substantial market share in many sectors, and they can heavily influence things, I find it hard to believe that the standards bodies will just roll over and accept whatever Cisco puts on the table. This is why companies use rhetoric like "pre-standard", because they know that there may be modifications. The real issue that people need to be aware of is whether the modifications to meet the eventual standard are just software tweaks that can easily be hidden in maintenance releases, or they require hardware updates that often can be expensive in purchase cost and upgrade time and effort.

Anon

SOMEONE HAS TO do the running, and Cisco has a track record of bringing innovation to networking as a whole, with a large part of that becoming part of or the basis of a standard.

If not Cisco then who would carry that banner — and if another did why would they be loved any more than Cisco?

In my view Cisco is not perfect, but they are good at producing a product that you can depend on, with support and training to match. Those who talk of a premium should look carefully at the support they get from other vendors outside of standard operating hours, and the time to replace a failed kit. When it comes down to it you get what you pay for — and I prefer to pay for 100% uptime, not gamble on it.

Anon

CONTACT US

Network World
492 Old Connecticut Path
Framingham, MA 01701-9002
(508) 766-5301
E-mail nwnews@nww.com

Subscriptions (877) 701-2228
URL www.subscribenww.com
E-mail nww@omeda.com

Reprints (717) 399-1900

NETWORKWORLD

CEO: Mike Friedenberg
GROUP PUBLISHER: Bob Melk (415) 975-2685
CHIEF CONTENT OFFICER/SVP: John Gallant
EDITOR IN CHIEF: John Dix

News
ONLINE EXECUTIVE EDITOR, NEWS: Bob Brown
ONLINE NEWS EDITOR: Michael Cooney
ONLINE NEWS EDITOR: Paul McNamara
ONLINE ASSOCIATE NEWS EDITOR: Ann Bednarz (612) 926-0470

Net Infrastructure
SENIOR EDITOR: John Cox (978) 834-0554
SENIOR EDITOR: Tim Greene
SENIOR EDITOR: Ellen Messmer (941) 792-1061
MANAGING EDITOR: Jim Duffy (716) 655-0103

Enterprise Computing
SENIOR EDITOR: Jon Brodkin

Application Services
NATIONAL CORRESPONDENT: Carolyn Duffy Marsan, (317) 566-0845

Service Providers
SENIOR WRITER: Brad Reed

Print Layout/Web Production
MANAGING EDITOR: Ryan Francis
COPY CHIEF: Tammy O'Keefe

Design
EXECUTIVE ART DIRECTOR: Mary Lester
ASSOCIATE ART DIRECTOR: Stephen Sauer

Features/New Data Center Supplements
EXECUTIVE FEATURES EDITOR: Neal Weinberg

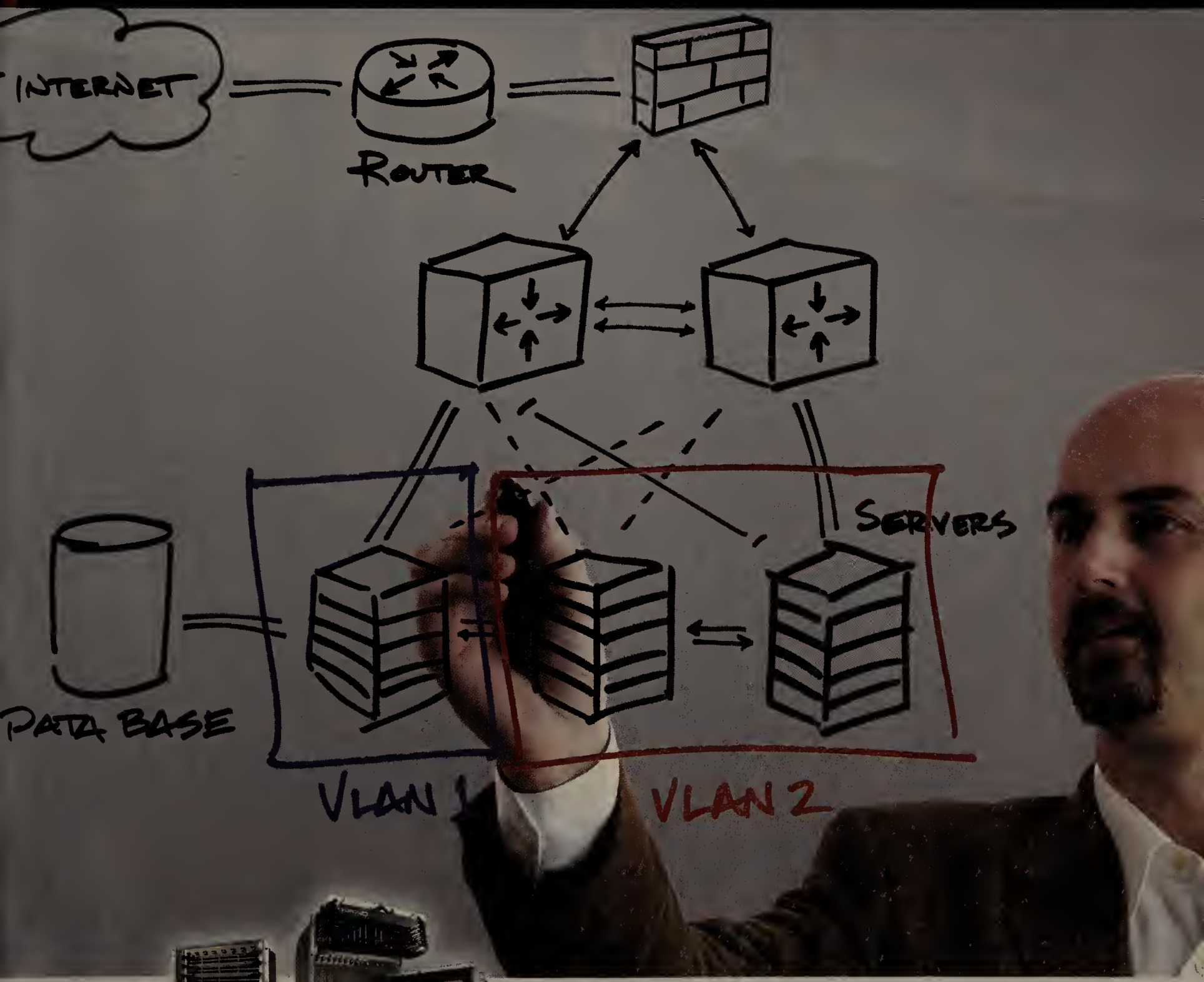
Clear Choice Tests
EXECUTIVE FEATURES EDITOR: Neal Weinberg
LAB ALLIANCE PARTNERS: Joel Snyder, Opus One; John Bass, Centennial Networking Labs; Barry Nance, independent consultant; Thomas Powell, PINT; Miercom; Thomas Henderson, ExtremeLabs; Travis Berkley, University of Kansas; David Newman, Network Test; James Gaskin, Gaskin Computing Services; Craig Mathias, FarPoint Group
CONTRIBUTING EDITORS: Daniel Briere, Mark Gibbs, James Kobielus, Mark Miller

networkworld.com
EXECUTIVE ONLINE EDITOR: Jeff Caruso, (631) 584-5829
COMMUNITY EDITOR: Julie Bort, (970) 482-6454
PROGRAMMING DIRECTOR: Keith Shaw, (508) 766-5444
EDITORIAL OPERATIONS MANAGER: Cheryl Crivello
OFFICE MANAGER, EDITORIAL: Pat Josefek
MAIN PHONE: (508) 766-5301
E-MAIL: firstinitiallastname@nww.com

OPEN AUTOMATION

Freedom of choice...ensuring the cloud works for you.

For more info see **force10networks.com**

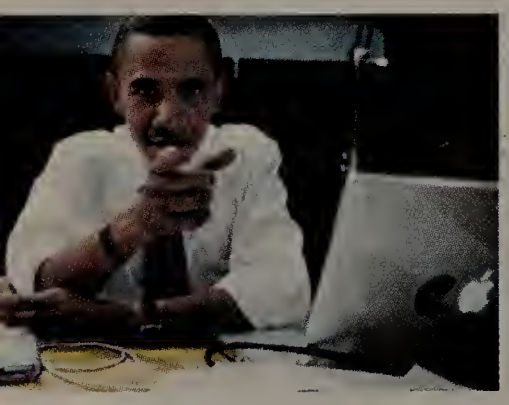


FORCE10™

When your network is your business.

Google on buying binge

NO LONGER CONTENT to watch Microsoft, Cisco and IBM dominate the technology M&A marketplace, Google has spent the first half of the year snapping up more venture-based start-ups than any other company. As July began, Google announced its intention to acquire ITA software, a maker of air travel flight information technology, continuing a blistering pace that has seen the company purchase about 20 companies in the past 12 months. As Google steps up competition against Microsoft and Apple, it is increasingly purchasing technology and key talent from start-ups, rather than developing it in-house, says Scott Austin, the editor of Dow Jones VentureWire. "They have a lot more competitors, and they need to stay acquisitive to compete," he says. ***tinyurl.com/3yv6trr***



White House neglecting cybersecurity R&D: report

GOVERNMENT RESEARCH and development aimed at bolstering cybersecurity is not getting the attention it requires from the White House Office of Science and Technology Policy (OSTP), according to a 35-page report by the Government Accountability Office. The OSTP was first tasked with creating such an R&D strategy in 2003. Over the years, the OSTP has taken "initial steps toward developing such an agenda," the GAO report said. However, "one does not currently exist" even today, the report said. ***tinyurl.com/3ac24q3***

400 iTunes customers singing fraud blues

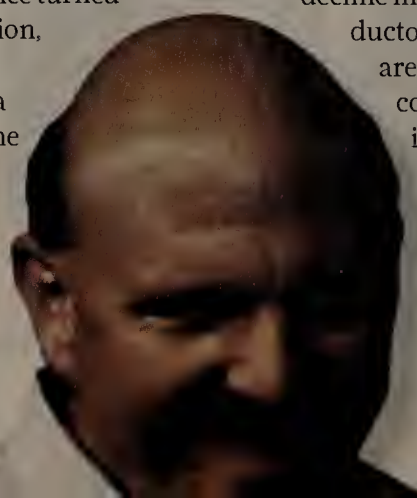
APPLE HAS banned a developer from its App Store after fraudulent purchases of his applications were made from around 400 accounts. Thuat Nguyen and his apps, which at one point reportedly occupied 42 of the top 50 positions in the book sales chart, was "removed from the App Store for violating the developer Program License Agreement," Apple's Trudy Muller said. "The iTunes servers were not compromised." Apple advised users who suspected fraudulent purchases were made to contact their bank and cancel the credit card in question. Apple also said users should change their iTunes password. ***tinyurl.com/3y9736v***

Amazon.com. groceries?

AMAZON.COM HAS launched a grocery delivery service in the U.K., following the recent kickoff of a similar service in Germany. The online retailer said it has 22,000 product lines ranging from cleaning products to fresh fruit to beer and pet food. Items that Amazon directly fulfills will be delivered in the mail. Customers have two options for delivery. For an annual $73.50 fee, customers can subscribe to Amazon's Prime membership, where an unlimited number of items can be delivered free. Another option is Free Super Saver delivery, which takes between three to five days after items are dispatched. ... Maybe not the best option for seafood. ***tinyurl.com/34eg9rj***

He's baaaack: Ballmer to headline CES

RUMORS ABOUT Microsoft CEO Steve Ballmer speaking at Apple's Worldwide Developers Conference turned out to be fiction, but Ballmer will deliver a keynote at the mammoth CES show in January. The Consumer Electronics Association announced last week that Ballmer will give the preshow keynote address on Jan. 5 in Las Vegas, just as he did earlier this year. At the 2010 CES, Ballmer showed off a few Windows 7 slate PCs, including one made by HP. HP ultimately dropped Windows 7 from its Slate tablet, however, so Ballmer will hope to make a product announcement with a little more staying power at next year's CES. In past years, Microsoft has also used the CES stage to announce the Xbox and Windows Vista. ***tinyurl.com/2vxvdsj***



Chipper outlook for chips, says IDC

AFTER SEEING chip sales decline in 2009, the semiconductor industry's fortunes are looking brighter in coming years, according to IDC. Worldwide chip sales slipped 9% in 2009, to $225 billion, but demand is stronger now and chip sales are expected to grow

1 YEAR FOR FREE!*

You spoke, we listened. With over 1,000 in-house developers, 1&1 has been working hard to create feature-packed website plans to meet the needs of even the most demanding web professional.

1&1® FREE HOSTING PACKAGE

- 2 Domain Names Included (.com, .net, .org, .info or .biz)
- 150 GB Web Space
- UNLIMITED Traffic
- 10 FTP Accounts
- 25 MySQL Databases (100 MB)
- Extensive Programming Language Support: Perl®, Python®, PHP 5/6 (beta) with Zend® Framework
- 1,200 E-Mail Accounts (IMAP/ POP3)

1 YEAR FREE

After the 1st year, pay just $6.99 per month*

1&1®

MEMBER OF united internet

Get started today, call 1-877-GO-1AND1

www.1and1.com

*Offer valid as of July 1, 2010 and applies to the Home Package only. 24 month minimum contract term and setup fee of $4.99 apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are tradema rks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

GOOD | BAD | UGLY

Security freebies

good

ACCORDING TO a new study, lots of people are using free security software. Opswat, which sells a development toolkit used to manage third-party security apps, concluded in its study that despite high brand awareness for companies such as Symantec and McAfee, their security software does not necessarily dominate the market in terms of installations. Forty-two percent of the market is composed of free products, according to the report, which focused on endpoint security software. Opswat gathered the data from Windows users running AppRemover, an application designed to completely uninstall security applications, and Am I Oesis OK?, which can detect whether security applications are compatible with other third-party applications.

Are you a snoop?

bad

IN A survey of IT professionals, 67% admitted having accessed information that was not relevant to their role, and 41% admitted abusing administrative passwords to snoop on sensitive or confidential information. The survey was conducted by security firm Cyber-Ark Software, which earlier this spring asked 400 IT professionals from the United States and the United Kingdom questions about snooping. About 245 IT professionals answered: "Have you ever accessed information on a system that was not relevant to your role?" and "Have you or any of your colleagues used the admin password to get at information that is otherwise confidential or sensitive?"

AT&T points the finger

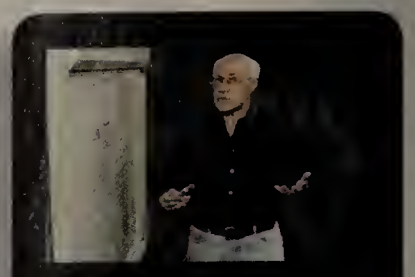
ugly

HEAVY DEMAND for upload capacity from the iPhone 4 has exposed a flaw in the software for Alcatel-Lucent's 3G network equipment, temporarily forcing lower upstream speeds for some AT&T subscribers. Alcatel is working on fixing the bug and expected last week to know soon when it will be fixed, according to a company spokeswoman. The flaw did not cause problems until the introduction of the iPhone 4, which comes with features such as high-definition video that can require a fast connection from the phone up to the network, she said. Downstream performance is not affected. Because the problem only exists in areas where AT&T uses Alcatel equipment, it affects only about 2% of the carrier's mobile subscribers, said AT&T spokesman Mark Siegel.

at a compound annual rate of 8.8% through 2014, the research firm said. "Order rates are now normalizing after very exuberant rates in the fourth quarter of 2009 and the first quarter of 2010," IDC said. Worldwide sales will hit $274 billion in 2010 — an increase of 22% over the previous year — and grow to $344 billion in 2014, the firm said. ***tinyurl.com/32v8efj***

Trade group warns of 'Net tax bill

THIS ISSUE has been around as long as the Internet. A new bill before Congress that would require Internet sellers in many states to collect sales tax would hurt small businesses online, a tech trade group said last week. The Main Street Fairness Act, introduced recently by Rep. Bill Delahunt, D-Mass., would allow states to force online sellers to collect sales tax, even if the seller has no physical presence in the state. Under current U.S. rules, Web sites must charge a tax on sales only when the customer is in a state where the seller has a physical presence. "Given the current economy, it would be unfair and unwise to burden online vendors with the task of sorting through the policies of thousands of taxing authorities around the country, and serving as revenue collection agencies for each of them," said the Computer and Communications Industry Association (CCIA). ***tinyurl.com/3y7yw6a***



IT Video

60 GHz and WiGig explained

Farpoint Group Principal Craig Mathias discusses the 60 GHz wireless spectrum and how it will open up new speeds for wireless transmission.
tinyurl.com/39dw7q2

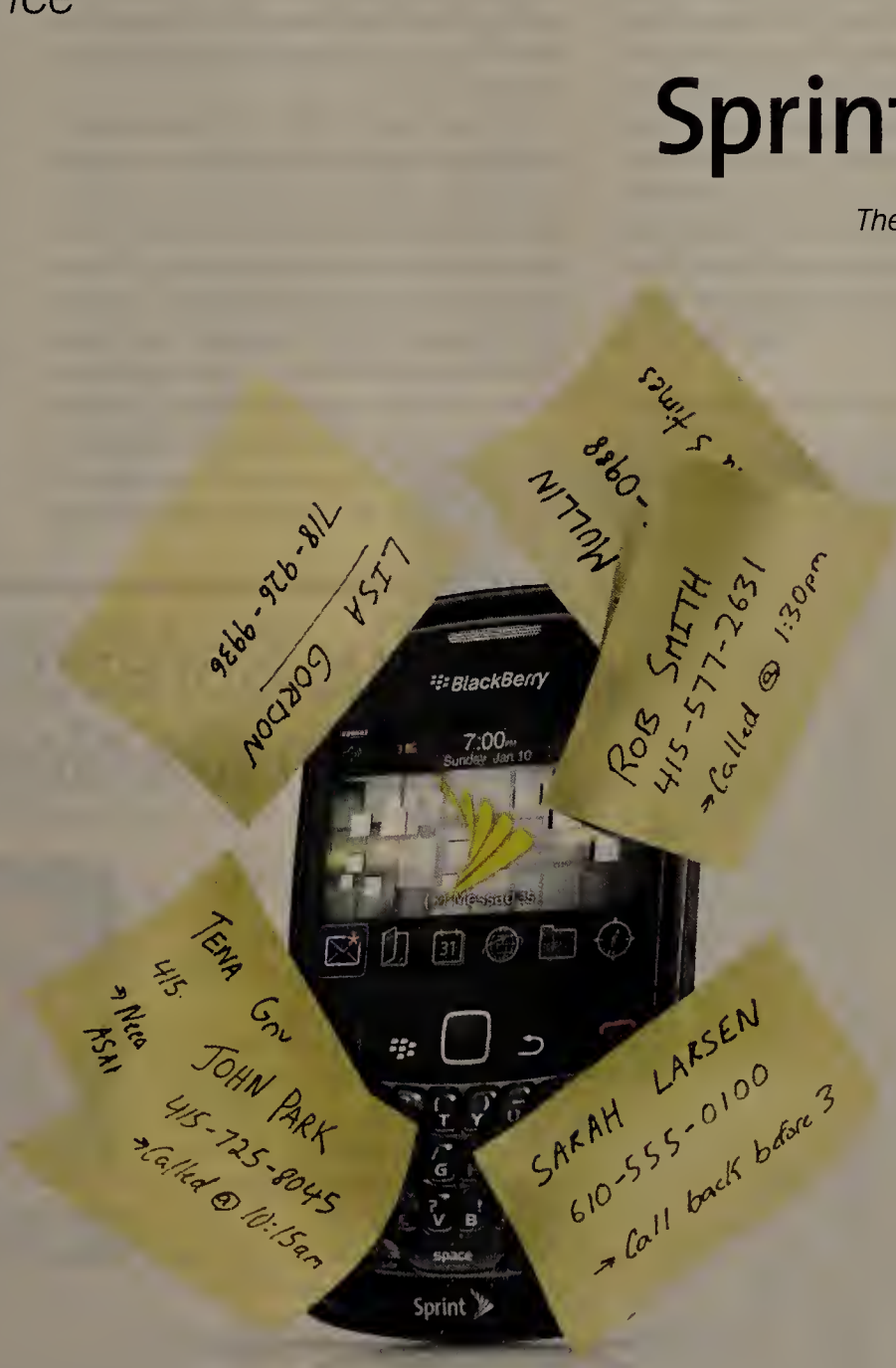
Nokia asks Russia for help; Apple can relate

NOKIA HAS asked Russian authorities to help retrieve what it says is an unauthorized model of a future phone that a blogger wrote about and photographed on a phone review site. (No word if Steve Jobs was advising the company or not.) Last week, Nokia wrote in a blog post that it had asked Russian authorities for help with the return of Nokia property in the possession of Eldar Murtazin, a blogger. In April, Murtazin wrote a brief blog post, in Russian, on the Mobile Review site that included photos of the N8. The N8, which will be the first phone to run the first open-source version of Symbian, isn't yet available. Nokia says that it formally requested the return of the phone from Murtazin but got no response. ***tinyurl.com/39bdz6x***

While you were out...

If you miss a call, you miss an opportunity. With Sprint Mobile Integration and Global MPLS, you'll have one number, one voicemail and one easy way to control mobile usage. Simplify the way your company stays in touch. Make it easier for clients to reach you. And reduce company telecom expenses. Less dialing, happier clients. Start closing. 1-866-653-1056
sprint.com/convergence

Sprint
The Now Network™



PilotHouse Award

IT professionals name Sprint best provider of MPLS—delivering best value, customer service, technology and network reliability.

Cloud computing providers working in secret

BY ELLEN MESSMER

DESPITE HOW attractive cloud computing can sound as an outsourcing option, there's widespread concern that it presents a security and legal minefield for businesses and government. Cloud service providers often cultivate an aura of secrecy about data centers and operations, claiming this stance improves their security even if it leaves everyone else in the dark.

Businesses and industry analysts are getting fed up with this cloud computing version of "don't ask, don't tell," where nondisclosure agreements (NDA) dominate, questions aren't answered, and data center locations and practices are treated like national security secrets. But public cloud service providers argue their penchant for secrecy is appropriate for the cloud model — and at any rate, everyone's doing it. They often hold out their SAS-70 audit certifications to appease any worry (though some don't have even that).

"The business data you store in Google's cloud is safe," said Google product marketing manager Adam Swidler at the recent Gartner security conference held in National Harbor, Md. He emphasized that Google's multi-tenant distributed model entails "splicing data across many hard drives" so that in this "hardened Linux stack" there's a "quick update of all fragments of all files in the hard drives," a process he called "obfuscated files."

Swidler acknowledged there has been some secrecy about where things are located because "we think it's a security risk." Nonetheless, "Google is trying to open up a little transparency in what we do," he said.

Currently, the information Google will disclose publicly or even under NDA won't satisfy everyone, Swidler acknowledged. "It's not enough for everybody. Some people do want to go deeper."

The location of data centers is a big issue in contract negotiations, where legislative and judicial issues abound. For instance, the location of data is an issue under some data-privacy laws, such as those from the European Union. But while customers often care about where their data is physically located, Google "believes this notion of where is data physically located is a bit antiquated," Swidler said.

Many disagree, however. Customers want to know where a cloud provider's data center is, says Kurt Jackson, managing director in a Pitney Bowes Insight division called OnDemand that offers software-as-a-service applications, such as maps for city services, to business and government customers.

The willingness of cloud provider Terremark to allow site visits and to discuss details about its data centers and its physical and network security was critical in the decision to use Terremark, Jackson says. "If you're running in Miami, you know you're in Miami," he says. "Some other providers just aren't as transparent."

The argument over transparency vs. secrecy in cloud computing is leading to a culture clash between the more traditional ways of handling data outsourcing and the newer cloud-computing utility methods and mindset.

Gartner analyst John Pescatore says it's simply not possible to know whether Google's technique of "hiding the data in a million places" is good security or not since there's no way to evaluate it. Speaking at the Gartner security conference, he said SAS-70 certification of any public cloud provider may be considered adequate for some customers, and not others. "SAS-70 is pretty meaningless from a security level, but it makes auditors happy."

Organizations with certain kinds of sensitive data are simply unlikely to find public cloud computing a right fit until the day comes when they can be sure their favorite security mechanisms are running in their cloud environment, Pescatore said.

Cloud computing challenges traditional notions about auditing and security, and it's possible a new way of auditing needs to evolve.

"If your service provider won't give you information about security processes and plans in order to do what's necessary, you shouldn't trust that provider," says Andreas Antonopoulos, an analyst with Nemertes Research.

The old idea of "security by obscurity," which suggests you can defend your security position best by keeping mum about everything, is misguided, he says. "It doesn't work. There's always someone who knows," Antonopoulos says. If you hear someone try to get your business by uttering that phrase, "run far and fast."

Analyzing the fine print

Legal experts took notice when the city of Los Angeles posted its contract with Google related to the city's migration to Google e-mail and collaboration services with the

Census Bureau counting heads in the cloud

BY CAROLYN DUFFY MARSAN

THE U.S. Census Bureau is singing the praises of cloud computing.

Census is taking advantage of several cloud-based computing services — from content delivery networks to hosted applications to free Web-based services— for its decennial survey.

Census CIO Brian McGrath

Census CIO Brian McGrath says the bureau has had a great experience buying software and infrastructure as a service, and that this approach has been an efficient and cost-effective way to meet the peak processing demands from the 2010 Census.

"We use the cloud in eight specific instances around the decennial survey," McGrath says. "That provided a huge benefit for us because we didn't have to stand up an infrastructure. We knew our requirements were for a definite period of time."

The Census Bureau's positive experience with cloud computing comes at a time when U.S. government agencies are being encouraged by Federal CIO Vivek Kundra to embrace cloud computing as a way of saving taxpayer dollars. Supporting Kundra's position, a recent Brookings Institute survey estimated that government agencies can save 25% to 50% by using cloud-based computing services instead of internal IT resources.

Industry observers say many agencies are interested in building their own private clouds.

"Fear of information being made available over the public Internet is keeping federal

► *See* **Census,** *page 12*

help of IT services firm CSC.

David Navetta, an attorney at Information Law Group, recently completed an analysis of the lengthy contracts with Google and CSC to determine how each side fared in defining responsibilities related to a potential data breach and indemnification of damages.

He note Google is defined in the arrangement as a CSC "subcontractor," and "therefore, as respects indemnification for a breach of confidentiality obligations or for lost City Data, CSC would be responsible to pay for Google's act or error." However, he thinks the term "lost data" should have been defined more clearly in the contracts.

Speaking in general about the job of evaluating and approving cloud services contracts, Navetta says it's common to encounter a rushed environment where cloud service providers insist they don't have time to discuss details and don't want to make changes.

"The usual line is 'we can't do this one change for one customer,'" Navetta says. Security and legal are typically "on the same side of the aisle," while the IT department wants to get something done quickly to save money. He says cloud providers often don't want to "let people truly look under the hood" and using them "constitutes a trade-off because you're losing control." Not surprisingly, large companies and government agencies can be expected to obtain more concessions from cloud-service providers.

But not all organizations have found they fret over contracts.

Lincoln Cannon, director of Web systems at Merit Medical Systems, says the manufacturer has taken a few steps into cloud computing with Google Apps and Telania's eLeap for sales training, as well as Amazon for development work related to a new corporate Web site.

The providers' boilerplate legal agreements were given to the legal department, which redlined them and went back and forth until both partners were satisfied, Cannon says. "The legal team was perfectly happy with Google Apps," he says. The most concern over cloud computing probably came from the CIO because of his data-protection responsibilities related to Sarbanes-Oxley regulations, Cannon says.

Not all cloud service providers harp on secrecy, either.

Cloud infrastructure services provider ReliaCloud has two data centers in the Minneapolis/St. Paul area, and has about 100 cloud customers using its new VMware-based environment built on a management platform designed by Cloud.com, says CTO Jason Baker.

However, most of the hosting provider's 5,000 customers continue to use the more traditional method the firm offers that entails use of dedicated servers in cages, Baker says. The idea of cloud computing is still very new and customers are trying to understand what's different. But Baker says he's convinced a shared-tenant virtual-machine-based cloud service carries some inherent security attributes in terms of high availability that can't be matched by dedicated servers.

"It's more reliable," he says. "If your application is running on one physical box, the customer would experience downtime. But in a cloud, we have a pool of virtual machines, and if one physical node goes down, we would automatically start somewhere else in the cloud." In addition, he says, use of some APIs in the future could allow customers' applications to sense when an increase in computing power is needed and execute that at once.

Unlike some cloud providers, Baker is willingly to tell you about security defenses in use, such as the Cisco ASA firewall.

The question for customers is how far the public cloud providers are going to pull back the kimono, says HP's chief security strategist Chris Whitener. "You should sort of insist on that," he says. ■

Inside the cloud security risk

While cloud computing offers many benefits, it can also create numerous information security risks. A report issued by the watchdogs at the Government Accountability Office found these threats to federal agency and consequently private and public enterprise cloud projects:

CONTROLS: the possibility that ineffective or non-compliant service provider security controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information.

LOSS: the potential loss of governance and physical control over agency data and information when an agency cedes control to the provider for the performance of certain security controls and practices.

BAD APPLES: the insecure or ineffective deletion of agency data by cloud providers once services have been provided and are complete; and potentially inadequate background security investigations for service provider employees that could lead to an increased risk of wrongful activities by malicious insiders.

SHARED GOODS: Multitenancy, or the sharing of computing resources by different organizations, can also increase risk because one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information. Another concern is the increased volume of data transmitted across agency and public networks. This could lead to an increased risk of data being intercepted in transit and then disclosed.

► **Census,** *from page 10*

agencies from wanting to use the public Internet as the cloud," says Susan Zeleniak, group president of Verizon Federal. "They're going to want to use private clouds. That's what we see more."

Census said it spent $11.8 million altogether on the eight cloud computing efforts that supported the 2010 Census.

In January, Census began using Akamai to enhance the performance of its redesigned Web site — www.census2010.gov — which features video clips, blogs and other interactive content aimed at citizens. The new Web site attracted 4 million to 5 million hits a week at its peak, about double the traffic of the bureau's legacy Web site — www.census.gov — aimed at statisticians.

"For our new Web site, we went to the cloud," McGrath says. "We went with an infrastructure-as-a-service solution, and what a great experience that was. We contracted with Akamai to use their CDN... At the peak of our usage, we were servicing somewhere around 85% of our content from the edge, and it was not even coming back to our infrastructure."

McGrath says using the Akamai network provided a better Web experience to citizens for less money than building their own network. Akamai also provided a barrier against distributed denial-of-service (DoS) attacks.

"That was a huge concern for us that in the height of the decennial activity if we were a target of a [distributed] DoS attack or the site would go down or the performance would go down that it would reflect negatively on the Census Bureau and deter citizens from participating," McGrath says. "Using the CDN was a huge positive lesson."

Census also used several software-as-a-service (SaaS) providers, including RightNow, which provides self-service customer support such as searchable FAQs. Census says it was able to get RightNow up and running 25 days after purchasing the system. Census says it would have taken six months just to select the IT infrastructure required to run the application in-house.

Census uses GovDelivery, which provides outsourced e-mail delivery services to public sector clients. GovDelivery's built-in blogging tool was used by the Census Bureau director to publish a blog within days of buying the service.

The bureau's Integrated Partner Contact Database is built upon Salesforce.com's platform, which it paid for on a subscription basis. Census was able to tweak the configurations on the Salesforce.com software, rather than having to conduct any custom programming.

Census also uses the free Google Map's API to quickly develop mapping applications including an assistance center lookup and an interactive road tour.

To speed up acquisition of these cloud-based services, Census partnered with other federal agencies including the National Institutes of Standards and Technology (NIST) and chose SaaS vendors that had already been certified by another agency. NIST is leading a federal cloud computing advisory council that is setting cloud standards and certifying cloud-based service providers to make it easier for agencies to buy cloud computing services.

"We didn't have to re-certify and re-accredit the systems, and it really pushed the delivery of the service down from months to days or weeks," McGrath says.

McGrath says the bureau is looking to expand its use of commercial cloud-based computing services where appropriate, and is also leveraging its experience with these vendors to build the Census private cloud.

"We have a pretty aggressive internal cloud effort that we are building out," McGrath says. "There are still some concerns about the security in the public cloud. I have every confidence that those will work out in coming years. For us, [the plan] is to leverage the efficiencies of cloud technology and build an internal cloud."

One reason Census can move so aggressively into cloud computing is that it has been migrating to virtualization over the last 18 months. As of June, the agency had 427 virtual machines running on 57 server platforms. Census uses VMware as its virtualization platform. The bureau says it has spent $6.1 million on the hardware and software for its Windows virtual farm.

"We've highly virtualized our Windows environment," McGrath explains. "We've gone from a model where we had one application on one server. Now we've got hundreds of guests in our virtual farms, and we are realizing significant savings of $2 million a year because we've compressed down our hardware footprint."

Next up for Census is virtualizing its Linux servers, which are standardized on RedHat. "We're doing a cost-benefit analysis," McGrath says. "It looks like of our 1,000 Linux servers, 80% are very good candidates for virtualization because they are probably running at 20% utilization or less."

Census also is looking at homogenizing and virtualizing its storage platforms, which contain more than 2.5 petabytes of data from the decennial census and other regular economic surveys that the bureau conducts.

"Virtualization is a piece of the overall cloud architecture," McGrath says. "It's a logical first step because what it allowed us to do is to really show in a limited investment, in a limited scale, the benefits of the cloud...We've been able to demonstrate to our customers that we are able to reduce our footprint, we're able to provision services more efficiently with less operations and maintenance costs, and our security costs are reduced because we can do security at the architecture level." ■

SIP trunking: A primer

How connecting your IP PBX to a SIP trunk can save serious cash

BY BRAD REED

TDM TRUNKS have long served to connect corporate PBXs to the public switched telephone network. But with more companies moving to VoIP, SIP trunking has become an increasingly popular technology companies can use to simplify their network architecture and save money. Here are the basics:

Just what is SIP trunking?

Let's take it one part at a time. SIP refers to Session Initiation Protocol, the standard developed in the 1990s by the Internet Engineering Task Force that is used to set up and terminate VoIP calls and generate dial tone. A SIP trunk, then, is a broadband Internet link that utilizes SIP to connect a company's IP-based PBX to an Internet telephone service provider (ITSP). Instead of terminating the trunk directly at the IP-PBX, for security sake companies tend to terminate the trunks at a SIP-capable session border control system that acts as a firewall.

How does a SIP trunk save money?

SIP trunking saves money by drastically consolidating and simplifying your voice architecture. SIP trunks can support voice, data and video all over IP, meaning a single trunk can replace multiple TDM trunks.

"If you have multiple offices and have a highly distributed network, you're probably going to have a lot of TDM trunking going into those organizations," says Michael Leo, of Acme Packet. "With SIP trunking you can reduce your traditional amount of TDM connectivity by better utilizing connectivity across the board."

SIP trunking also makes it possible to add capacity during times of high call traffic. If you rely on T-1 lines, for instance, you have to purchase 24 channels even if you only use five of them at any given time. With SIP trunking, if your provider supports the capability, you just assign bandwidth to locations as needed to deal with high call volume. "Without SIP trunking you have to buy extra lines and pay for them all year whether you need them or not," says Nemertes Research analyst Irwin Lazar. "With SIP trunking you can burst call access during special times."

How much money can it save?

Lazar estimates that on average companies that adopt SIP trunking save 20% to 60% from what they pay now for TDM trunks. Citing one case study, Leo from Acme Packet says he knows of one company that used 1,500 SIP trunks to replace 2,250 trunks, a shift that reduced telecom expenses from $5.4 million per year to $945,000 per year.

What questions should I ask a SIP trunk service provider before investing?

The big one is simply whether SIP trunks will be available for all your branches. As Leo notes, businesses with offices in rural or remote areas could have difficulty finding a vendor that covers all their locations: "As service providers ramped up they have addressed large metropolitan areas first. But when you get to more remote locations it's lagging behind. It's only been in the last two years that SIP trunking has become available to enterprises."

The second big question has to do with interoperability, as many SIP trunking providers will only support a limited number of vendors. In other words, some SIP trunk providers may only support session border controllers from Avaya while others might only support session border controllers from Cisco.

And finally, you'll want to ask about pricing schemes, both in terms of overall installation costs and flexibility to quickly and affordably add capacity. Because SIP trunks are still a relatively new technology, they don't really have standardized pricing schemes and can vary widely in the services they provide.

"You'll definitely want to ask them how quickly they can get a SIP trunk up and running," says Anne Coulombe, an Avaya executive. "Some of the tier-two service providers are extremely rapid in being able to ramp up SIP trunks, while the big carriers are a little slower."

Is there any business where a SIP trunk is not worth the investment?

SIP trunks provide the most efficiency for businesses that have multiple locations spread out over a wide area. If you only have one central location, or if you have offices that are located in a very concentrated geographic area, then a SIP trunk will probably not be worth your time.

"If you're a company that's already oriented toward TDM and most of your calls go between one or another town, then you might not need SIP trunking," Coulombe says. "So a pharmacy with only two branches might not need it, but if that pharmacy grew to have 15 branches then SIP trunking would be really worthwhile for them." ■

Poor SSL set-up can kill e-commerce

Black Hat talk will show how poor SSL implementation can hurt online business

BY TIM GREENE

ONLINE MERCHANTS are shooting themselves in the foot with faulty SSL deployments that trigger alarms scaring customers away before they have the chance to complete transactions.

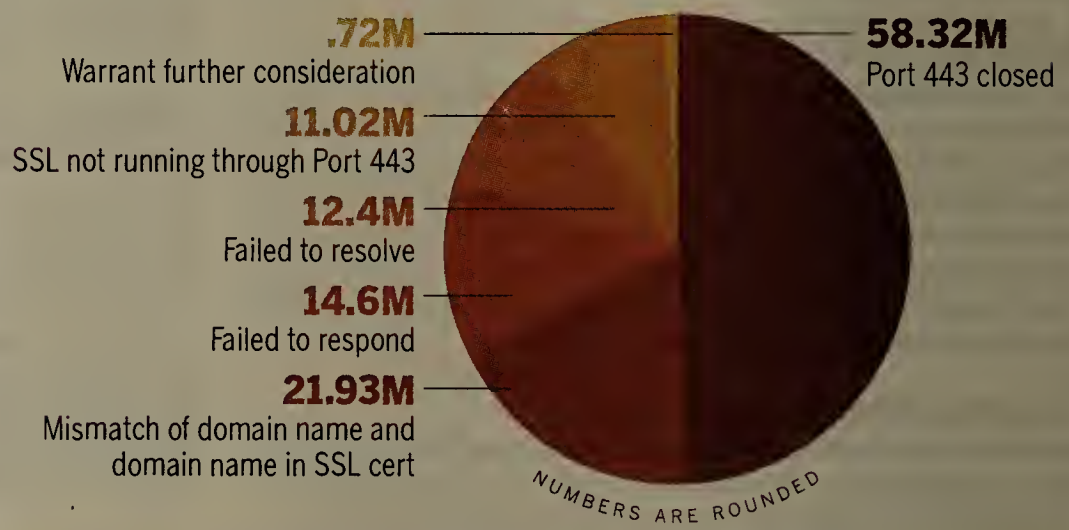
The problem is not with SSL technology, but with factors surrounding its implementation that hurt security or the perception of security, either of which can undermine customer trust, says Ivan Ristic, director of engineering, Web application firewall and SSL services at Qualys, who will present "State of SSL on the Internet: 2010 Survey, Results and Conclusions" at the Black Hat 2010 conference later this month.

Notable among the problems is the mismatch between the domain names listed on SSL certificates and the domain names of the merchants, he says. This mismatch triggers browser popup warnings that the certificate may be invalid, and at that point potential customers may choose to bail out of transactions, Ristic says. "We are creating a sense of fear among customers that there are problems around every corner," he says. "Technically, SSL is a very good protocol. The way we use it today is not very good."

At Black Hat, Ristic will reveal the results of an extensive study he has led about usage of SSL and its newer incarnation Transport Layer Security (TLS) with the aim to address problems that appear on Internet sites. He is still crunching the numbers from his yearlong survey of Web sites, but has a sense of prevalent issues. "There is some evidence that 50% of all SSL problems are due to misconfiguration and do not come from any vulnerabilities as such," he says.

SSL done wrong

Researcher Ivan Ristic will tell Black Hat 2010 that after eliminating domain names for a variety of reasons shown here, he has come up with comparatively few that support SSL properly.



In many cases, once users recognize the shortcomings of their implementations, they could fix them in an hour or so, greatly improving site overall security.

He says his talk will focus on three areas: the certificates; which version of SSL is used; and configuration weaknesses in type of Web server, cipher suites and protocol support among others. The survey looks for sites using known insecure versions of SSL that should have been replaced and other bad practices that undermine security, he says.

The goal of research by SSL Labs is to find best practices among real SSL sites. So far, the study has tried to find as many SSL servers as it can on the Internet, and Ristic decided to do so by connecting to as many of the 193 million registered domain names as possible. He readily got all the .com, .net, .org, .biz, .us and .info names, which gave him the 119 million he started with.

Then he weeded out the ones that looked unpromising — those that failed to resolve (12.4 million) and those that failed to respond (14.6 million). Of the remaining 91.65 million, only 33.69 opened Port 443, which is designated for SSL. Of those, 22.65 million were actually running SSL through the port.

According to SSL Labs' criteria, certificates with domain names that don't match the sites' domain names should be considered invalid, ruling out another 21.93 million. That left just 719,093 SSL sites worth considering further to find out how to do SSL right, he says.

The expense of setting up SSL sites through Web hosts may also be a factor in bad implementations, Ristic says. Businesses that want to process customer transactions online need SSL, and if they want to use their own SSL certificates that feature their domain names, they also need unique IP addresses. There are hosting services that share SSL certificates among customers, but these will run into the problem of the certificate domain name not matching the business domain name.

Hosting SSL servers on virtual machines as part of hosting providers' services is needed to drop the cost of properly carried-out sites, Ristic says.

Improved online sales also depend on performance of SSL sites, and that performance will be the subject of later reports by SSL Labs, he says. The current report will tap more than 300 factors that an automated scan of SSL sites performed on the sites SSL Labs deemed worth pursuing.

The test gleans information about the domain common name, alternative names, revocation information, the certificate chain, validation, flavors of SSL and TLS supported and whether the domain supports secure and insecure renegotiation.

Each scan takes 5 to 50 seconds depending on network latency, and the gear being used can run 500 tests in parallel, completing about five per second, he says. ■

RISKANDREWARD | BY ANDREAS ANTONOPOULOS

Honeypots for hacker detection

MOST CORPORATE networks lack serious oversight, that is, no one is really watching. Watching the network and computer systems is expensive, overwhelming and fraught with false positives. No wonder then that insider attacks go undetected for months, malware proliferates stealthily and hackers can spend their time gradually infiltrating deeper and deeper, undetected. It's simply too hard to discern between legitimate activities and illegitimate or malicious activities. Without context, wading in the enormous volume of logs or network traffic leads to information overload. How to tell who's up to no good? Well, you shall know them by their deeds.

Honeypots are an underutilized tactic. Every attack has an exploratory component. When hackers or viruses go probing networks and systems they are usually able to do so unnoticed. Unless they cause a system crash or overwhelm a system, the chances of detection are pretty low. A honeypot is a system that detects unusual activity by creating false targets. In a network, for example, a simple honeypot may allocate the unused IP address space. Then if someone attempts to access an IP address that is not used, an alert can be generated. Similarly, a port-based honeypot could respond to requests on unused TCP ports, creating the illusion of services. Entire computers, or even networks of computers, can be created to lure attackers.

Some may object to the use of honeypots because they might be seen as "entrapment" under the law. I'm recommending the use of honeypots for detection and prevention of attacks, not prosecution. If someone is accessing a system that has no DNS name, no public or registered services, no legitimate function, then it is quite likely that they're up to no good. Alerting on such access can give security professionals advance warning of attacks with fewer false positives. Of course, there are network diagnostic tools and other management tools that probe entire networks, but it is not very difficult to exclude those. Honeypots can even automate intrusion prevention by temporarily blacklisting IP addresses, thereby acting as booby traps for attackers.

I've applied this tactic successfully on both personal and corporate networks. What perplexes me is that there are so few vendors offering honeypot-like solutions in their products as a standard security feature. Network equipment (routers and switches) could offer phantom honeypot networks that generated alerts. Virtualization software could create entire phantom honeypot data centers. Service providers could use honeypots on unallocated network space. Sophisticated honeypots can even "lure" attackers by creating the illusion of success and escalating the intrusion, profiling the attacker all the way (see www.mykonossoftware.com for one example of this tactic).

There are very few legitimate reasons to go probing in the dark recesses of most networks, operating systems or applications. Honeypots give us an opportunity to set traps in those spaces, making an attacker's exploratory forays risky and more likely to be detected. A mirage of fake systems can waste attacker's time, giving us a head start in detecting, identifying and thwarting them. That's how you catch hackers with honey. ■

Antonopoulos is a senior vice president and founding partner at Nemertes Research, an independent technology research firm. He can be reached at andreas@nemertes.com.

TOOLS

Ctera brings the cloud down scale

Last week I reviewed the Alex e-book reader from Spring Design (tinyurl.com/3ac9xqw) and complained that the device didn't support PDF or text documents. I was foolishly relying on the product specs, which didn't mention anything about PDF documents. It turns out that the Alex can read and render PDF files, but here's the rub: The Alex can't "re-flow" the content in a PDF file.

Mark Gibbs' Gearhead

This is to say that when you zoom in because the text is too small, the text on each line isn't reformatted and wrapped to fit the screen. This means you have to scroll left and right and up and down to view the text.

Scrolling is something the Alex can do but it's tricky because you have to press the synchronize button so the PDF document shown on the large electronic paper display (EPD) up top is shown on the device's smaller touch-sensitive LCD display below. Then, using your finger, you move the image on the LCD, and the EPD display is updated to show the new position.

This is like using a remote control on a TV and makes for an experience that isn't much like reading a book. And when you leave the document, your zoom and position settings aren't retained so when you return you're back to the whole page view. This is hardly an adequate implementation of PDF viewing. I'm told a future update will address this. Even so, I still like the Alex.

Now onto the cloud, which is still the hot technology pin up. I last discussed the cloud when I reviewed Gadinet's desktop cloud storage tool some months ago.

I have another interesting network storage solution that is ideal for workgroup or small office/home office (SOHO) use: The Ctera C200, a $499 device that provides network-attached storage (NAS) services as well as storage-area network (SAN) services along with optional backup to Ctera's online storage services.

> I have another interesting network storage solution that is **ideal for workgroup** or SOHO use.

The C200 is a small (6.4 by 8.27 by 3.74 inch) device that consumes a measly 50 watts of power. It has two drive bays for 3.5-inch SATA drives, which can be hot swapped. Given that 3TB SATA drives are now available a C200 could, in JBOD (Just a Big Old Disk) configuration, provide 6TB which should keep even large workgroups happy for a long time. Alternative storage configurations include RAID0 (striped) and RAID1 (mirrored).

The C200 is configured through its Web interface. File sharing is supported through CIFS (Windows File Sharing), AFP (Apple Filing Protocol), Apple Time Machine, FTP, WebDAV, and good ol' rsync. Through client shares a so-called "clientless" backup is supported.

► *See* **Gearhead,** *page 17*

IT asked and answered

Ron Nutter tackles your tough tech questions at tinyurl.com/yg2o434

Our HR department has come to me with a request to block certain types of Web sites, i.e., file sharing, adult themed, etc. How much will a solution cost, how long to implement and what type of ongoing maintenance support is required/available?

Two solutions that come to mind are Websense and Smartfilter. These options will require you to set up a server for the application and make some minor changes to your firewall to point to the tool for go/no go decisions. In fact, I would start by checking the firewall to see what options are supported. If funds are tight I noticed this option that SANS posted - tinyurl.com/35gwj63. Basically it involves setting up a Linux server running bind with some configuration scripts. If you aren't familiar with Linux, don't worry, it isn't that hard to do. I set up a pair of bind servers for a small college so all requests from users on campus came through those servers but any DNS requests that came from the outside were met with a DNS Root hints message if the request was for a domain the college wasn't hosting. Once you decide on how you are going to proceed, make sure HR and Legal are both on board. It is a good idea to make legal aware of what is going on in case something happens. Keep good records to make sure you are protected, including a good e-mail trail from HR on their approval for the changes. Once this is all set up, establish a formal change process so there is a set path that has to be followed when any changes for Internet access are requested.

Uploading HD video wirelessly? Yes you can!

Keith Shaw's Cool Tools

A LOT HAS been written about the iPhone 4's ability to record HD video, and its inability to upload via the AT&T 3G wireless network (maybe next year, guys). However, there's another way you can record HD video and upload it wirelessly (via Wi-Fi), with the help of two cool tools:

THE SCOOP

DXG-A85V Pro Gear HD video camera and Eye-Fi Pro X2 8GB SDHC card

by DXG, about $320 and $150, respectively

► **What it is:** The DXG-A85V Pro Gear video camera offers a lot of the same features found in brand name video cameras, but without the brand name price. This model includes a 10 megapixel image sensor, 12x optical zoom, and can record videos with 1080p resolution at 30 frames per second, or 720p resolution at 60 frames per second. The DXG-A85V includes a 3-inch touchscreen display for easy menu option navigation, and an HDMI cable and interface for connecting to an external display. The system supports SDHC cards up to 16GB in capacity, and this includes the 8GB Eye-Fi Pro X2 model. Videos are stored in the .MOV file format.

► **Why it's cool:** The camera was very easy to use, the LCD screen pops out from the side, and the touchscreen was a nice and easy way to change resolution settings (we tend to shoot in 720p to save on file sizes). The dual-capture mode, in which you can record videos and pictures simultaneously, was a very nice touch. The electronic image stabilization feature was handy.

When you add the Eye-Fi Pro X2 card to the camera, you can automatically upload your videos and photos via Wi-Fi network to a photo sharing site. The card features its Endless Memory Mode, which automatically frees up space on the card once photos and videos have been uploaded. The card can also upload images and videos through AT&T Wi-Fi hot spots. But for the most part, you'll want to upload photos through your own Wi-Fi network at home, especially if you have an 802.11n network.

Using the Eye-Fi card was also a breeze; once configured it was a great way to quickly upload photos to Facebook and other photo sharing sites, and the software lets you choose privacy settings on photos, as well as choose only the photos you want to upload.

► **Some caveats:** On the camera, I would have preferred an external microphone jack, which can help in noisy environments. On the card, I have no complaints other than the sticker price — make sure that wireless uploading is something you plan to do frequently, otherwise you can pick up a regular SDHC for a lower price.

► **Grade** ★★★★½ (out of five) for each product.

Shaw can be reached at kshaw@nww.com.

The DXG-A85V is similar to brand name video cameras but at a lower price.

TRUE FACT

21 EXABYTES

Estimated global monthly Internet traffic

SOURCE: CISCO AN EXABYTE EQUALS 1 BILLION GIGABYTES

► **Gearhead,** *from page 16*

Ctera also provide an installable client for Windows XP, Vista and Windows 7 that can backup open files (unfortunately there's no support yet for server versions of Windows, OS X or Linux). Versioning is supported through both automatic and manual "snapshots".

Ctera makes it possible to have your C200 synchronize with Ctera's online backup service (the device also provides content encryption).

This is all easy to set up and manage, making it usable by organizations with limited tech support. The C200 comes with 5GB of online storage and is free for the first 30 days. After that subscriptions start at $9.95 per month for 10GB and go up to $99.95 per month for 200GB. You can also attach multiple devices (only C200s are currently available) to an account, which provides a simple, centralized management strategy.

But there are a few minor problems: the Web-based user interface has a few usability issues, there is no UPS support, and the event notification service doesn't support SMTP servers that require SSL or TLS secured connections. That said, these are minor in comparison to the range of features offered.

So that's it: A SAN, NAS and cloud storage solution that's simple to use, simple to manage and has very good performance, all at a reasonable price. The Ctera C200 gets a rating of 4.5 out of 5.

Gibbs has a clouded view. Your vision to gearhead@gibbs.com.

ndc
THE NEW DATA CENTER

The meteoric rise in virtualization and cloud computing has thrown traditional network security off its axis. New tools and approaches are needed in order to protect virtual machines and cloud-based data.

THE ISSUE STARTS NOW

The virtual blind spot

Virtual machine traffic presents a new challenge for data center security professionals

~ *BY BETH SCHULTZ* ~

Malicious hypervisors. Subversive virtual machines. Live migration impersonators. Welcome to the world of server virtualization, where the threats are new and the traditional security tools such as firewalls and intrusion-prevention systems (IPS) don't cut it anymore.

Unfortunately, at many enterprises, security strategies haven't kept pace with the shift to x86 server virtualization. "Many companies that have virtualized environments haven't contemplated the security ramifications of what they're doing yet," says John Kindervag, a Forrester Research analyst.

PATRICK QUINN

ASSISTANT VP OF THOMASTON SAVINGS BANK RELIES ON A TOOL FROM CATBIRD NETWORKS TO PROTECT HIS VIRTUAL SERVERS

Gartner's Neil MacDonald agrees. "The general awareness level of issues related to virtual security isn't quite where we need it to be," he says.

For their part, IT pros tend to look at it this way: Since physical and virtual servers run the same Linux and Windows operating systems on the same hardware, then security for the former is adequate for the latter. "They'll argue that nothing has changed — and that's a dangerous mistake," MacDonald says.

"When you virtualize, you introduce a new layer of software and all of the Windows and Linux workloads running on top of it rely on its integrity. The first and most important thing you need to do is acknowledge this new layer and establish basic security hygiene around the configuration and vulnerability management of it," MacDonald says. "That's basic block and tackle."

Secondly, IT needs to figure out what to do about the network blind spot that virtualization creates, he adds.

"None of our network-based firewalls or IPSs in the physical world can see the traffic being switched between two virtual machines (VM) in the same box," MacDonald says. "The question we need to answer is, 'Do we need security controls inside of the virtual server to see this virtual network traffic?' Maybe you do or maybe you don't – but you've got to acknowledge that you can't see the traffic and if something bad happens, like an inter-VM attack, you won't be able to see it."

Many enterprises haven't focused on virtual server security because their virtualization deployments are immature. When virtual servers are only used for test and development purposes or for running non-critical, low-priority applications, security doesn't much matter.

But that changes as a virtualization layer moves into the production environment to host mission-critical applications. The deeper entrenched virtualization becomes, the greater the need to deploy security technology specifically aimed at protecting the virtual infrastructure.

Awakening to a new reality

"We did originally go through a phase where we thought physical security would do. But as we started to grow our virtualization deployment, we felt we needed to make sure we were taking proactive steps to secure our customer information," says Patrick Quinn, assistant vice president and network administrator at Thomaston Savings Bank, in Connecticut.

In doing so, the bank set up secure network segments in the virtual environment much as it would do on physical infrastructure. It uses Catbird Networks' vSecurity TrustZones virtual security technology, which allows VMs of varying trust levels to share a common host.

TrustZones lets Quinn control traffic moving between VMs based on policy. For example, Quinn says he has established trust zones for each branch, as well as several for the main office.

Likewise, Interior Health Authority, a regional health agency in Kelowna, British Columbia, is hoping to incorporate a virtual server layer into its overall security architecture, says Kris Jmaeff, information security specialist.

"Definitely one of our goals is to have visibility within the virtualization layer," Jmaeff says. "We've got certain areas where we need to use virtual sensors to monitor traffic within our virtual server world or cluster."

Toward that end, Interior Health is beta testing HP TippingPoint's Security Virtual Framework, which lets security teams monitor vSwitch — the virtual switch within VMware's platform — and VM changes to identify tampering or disablement of security controls.

In addition, HP TippingPoint virtual IPS integrates with the vTrust virtual security technology from Reflex Systems. Similar to Catbird's TrustZones, the Reflex technology lets users create trusted network segments and enforce policies, as well as monitor, filter and control VM-to-VM traffic.

"Our goals for the beta test are to increase our knowledge, obtain more insight and visibility on infrastructure, and develop pre-engagement, pre-planning ideas of what we're going to do with security in the future. This is a good opportunity to learn and be on the cutting edge of virtual security," Jmaeff says.

Virtual security vendors step up

Catbird and Reflex are but two companies that are targeting virtual server security. Others include start-ups such as Altor Networks, Apani and HyTrust, as well as well-established security vendors. Besides HP TippingPoint, this latter group includes CA Technologies, for security functions such as access control and log management; Check Point Software Technologies, for virtual firewalls; Juniper Networks, which has a strategic alliance with Altor; IBM, for IPS; and Trend Micro, which acquired virtual security start-up Third Brigade.

"As bigger companies jump in, this signals that there is a need for these types of products. It's just a matter of time before they all have virtualized offerings of security enforcement," Gartner's MacDonald says.

It might seem logical to think that you would defend the hypervisor layer the same way you would defend physical servers — by plugging in IPS or antivirus software.

But MacDonald disagrees. "We don't believe you need to go run IPS or a copy of antivirus in the hypervisor. That would defeat the whole purpose of this layer being very thin and hardened. Rather, good configuration, vulnerability and patch management disciplines are enough at that layer," MacDonald says.

Forrester's Kindervag adds, "They say about 40% of issues in modern networks

STEVEN VOTE

relate to configuration or other types of human error. That leads me to believe that how you do security management is more critical [than hypervisor security] at this moment," he says.

"What vendors really are talking about now is protecting the VMs and traffic between them just as you'd protect workloads in the physical environment," MacDonald adds. "This becomes especially important when you start combining virtual workloads of different trust levels on the same physical servers. You're going to need that visibility, that separation and that policy enforcement."

When evaluating virtual security products, he advises, select those that are optimized to run inside the virtualization environment and have been integrated into virtualization frameworks from Microsoft, VMware and Xen-based virtualization vendors.

For its part, virtualization leader VMware gives virtual security companies visibility into VM operations via its VMsafe application programming interface.

"About seven major security vendors have participated as VMsafe partners. They've developed virtualization-aware network and endpoint solutions that work through the hypervisor in a privileged fashion with high security," says Venu Aravamudan, senior director of product marketing for VMware's server business unit.

But that's just for starters, he adds. Earlier this year, at the RSA Conference 2010, VMware previewed how it envisions next-generation virtual server security technology might work. Working in conjunction with Trend Micro, it showed the ability to run antivirus processing on a host machine rather than VM by VM as current-generation products do.

"Once this technology becomes real, in terms of a shipping product, we don't have the need for an agent in each VM. That means better performance, less to manage, lower cost and so on," Aravamudan says.

It also means new capabilities. "You can look at this model to drive solutions such as being able to detect rootkits in the files hypervisors are running on, discover credit-card and other sensitive information in VMs and check the integrity of files, for example," he says.

Baked-in security

Morgan Keegan & Co., one of the nation's largest regional investment firms, is one of the few companies quite comfortable with its virtual security posture. "We don't have any security concerns today in the way that we've deployed the virtual environment," asserts Luke McClain, a systems engineer with the Memphis firm.

Six tips for securing virtual servers

Forrester Research analysts suggest these policies will ensure a secure virtualization implementation:

- Manage virtual operating systems as you do ordinary ones. In other words, be vigilant about configuration, vulnerability and patch management in the hypervisor and guest operating systems.
- Segregate hypervisor and management interfaces, making sure that guest operating system virtual machines (VM) don't have access to the control mechanisms or even knowledge of the hosts on which they're running.
- Separate administrative and hypervisor traffic from production traffic.
- Continuously scan hypervisor hosts for — and harden them against — vulnerabilities.
- Don't mix VMs of varying trust levels on the same physical host.
- Don't rely on the hypervisor to enforce zone boundaries with a physical host. Rather, keep VMs from the same zone together.

That's because Morgan Keegan took security into consideration from Day One of its virtualization project, launched in March 2008. That the company already has virtualized 75% of its server infrastructure — roughly 515 VMs running on 52 VMware ESX hosts across three data centers — is in part attributable to this fact, McClain says.

A particular IT operational goal was collapsing the company's traditional firewalled DMZ into the virtual environment. "We felt that we could really benefit by bringing those physical machines into the virtual environment and manage them while still leaving them in this protected pocket," says Parker Mabry, managing director network systems engineering at Morgan Keegan.

This required close planning with the information security group, which compared virtual firewalls against what it knew of their physical counterparts — in its case, Cisco's firewalls. "They compared feature to feature, looking for things like robust logging, forensics and the depth and granularity of locking down machines," Mabry says.

"I like to tease that usually the first response we get from corporate information security is 'No' — it's that tight," he says. "So actually getting information security to see the value of being able to use a virtual firewall in the virtual environment was a big win for us."

To harden the virtual DMZ, Morgan Keegan uses Reflex's vTrust Security product.

From an operational standpoint, the company secures VMs through tight authentication, McClain adds. With VMware's vCenter virtualization management tool and the management interface, "We're very cognizant of who has rights to any virtual machine and keeping close track of that specifically and especially in the DMZ environment," he says.

VMware encourages its partners and field service organization to ensure that all enterprises bake security into their planning and designs, as Morgan Keegan has, Aravamudan says.

While the security-first encouragement doesn't always stick with customers just starting out on their virtualization journeys or who are using the technology in limited scenarios, larger enterprises do get it, he says.

"Especially at those customers with large percentages of workflows deployed on virtual servers, we clearly see a lot more discipline in adhering to our best practices and security hardening guidelines," he adds.

VMware believes that just as virtualization enabled massive cost savings and efficiency gains, it is a real game-changer when it comes to security, Aravamudan says. "It's definitely one of our goals — and we've already started to prove this — that security for environments based on virtualization will be better than physical security as it exists today in IT."

Gartner's MacDonald agrees. "What we see clearly is that virtualization is not inherently insecure, but that it gets deployed insecurely today. But this problem will go away over the next three to four years as IT staffs, vendors, the tools and skills mature," he says. "People will be deploying securely — ideally even more securely — than they have been in their physical environments." ■

Schultz, author of the Network World's *Network/Systems Management Alert, is a longtime IT writer and editor in Chicago. You can reach her at bschultz5824@gmail.com.*

YOU WANT A SAFE AND SECURE PLACE TO PUT YOUR CRITICAL CORPORATE DATA. WE KNOW. YOU WANT TO CUT COSTS AND ONLY PAY FOR THE SERVICES YOU USE. WE KNOW. YOU WANT A SCALABLE, GLOBAL SOLUTION THAT WILL ADAPT AS YOUR BUSINESS GROWS. WE KNOW.

Savvis Knows

SOLUTIONS FOR ENTERPRISE-CLASS CLOUD

Savvis Symphony is an industry-leading suite of cloud products for the enterprise, delivering real cost savings, high performance, reliability and security in a flexible, easy-to-use cloud interface. Combined with our global data center footprint and leading network connectivity, there is simply no better enterprise-class cloud solution.

SAVVIS KNOWS.

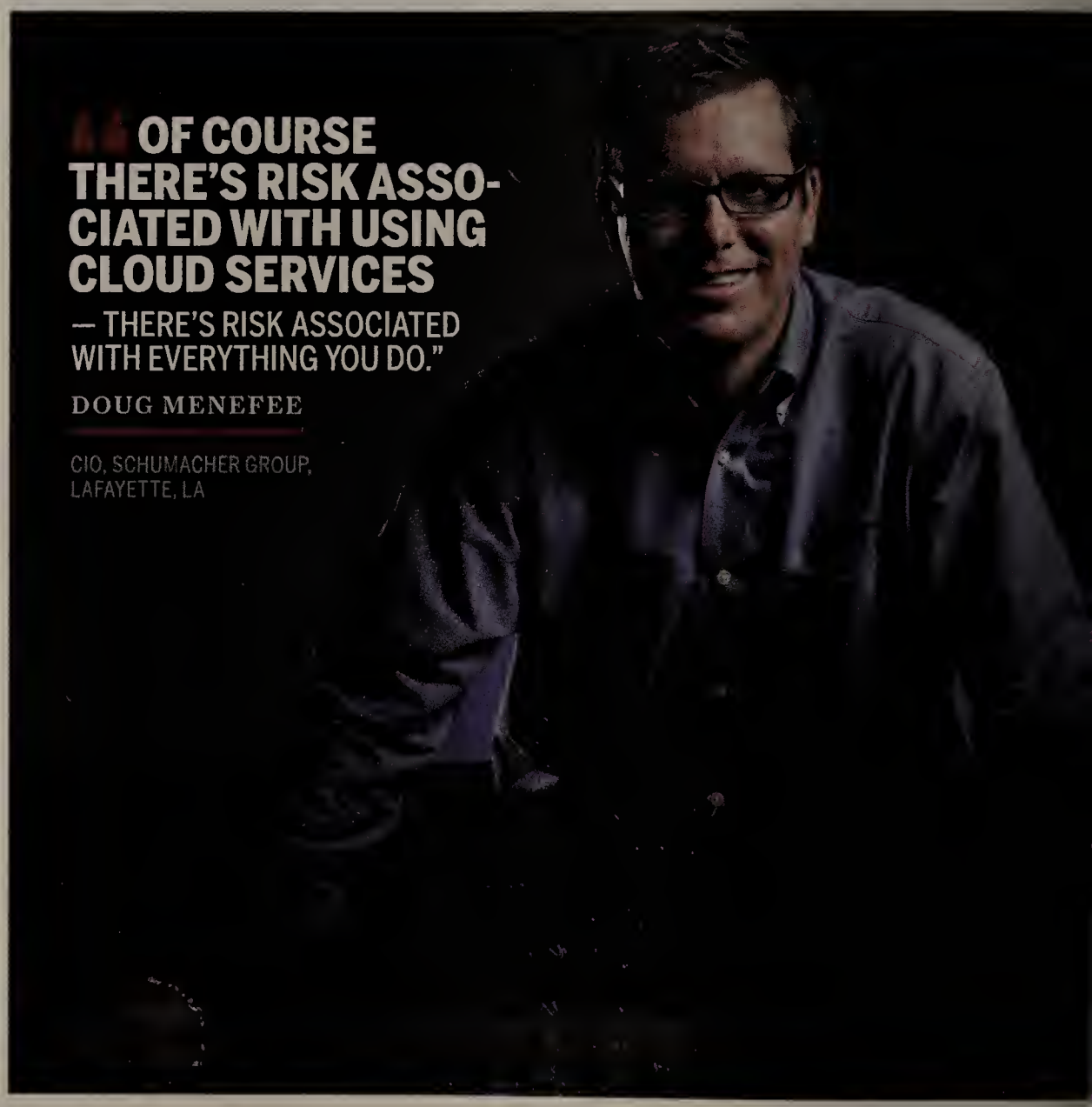
SAVVIS

Learn more.
savvisknowscloud.com
1-866-598-0800

How to secure the public cloud

New thinking and new tools are needed to securely run application workloads and store data in the public cloud

~ *BY BETH SCHULTZ* ~



Some IT execs dismiss public cloud services as being too insecure to trust with critical or sensitive application workloads and data. But not Doug Menefee, CIO of Schumacher Group, an emergency management firm in Lafayette, La.

"Of course there's risk associated with using cloud services — there's risk associated with everything you do, whether you're walking down the street or deploying an e-mail solution out there. You have to weigh business benefits against those risks," he says.

Menefee practices what he preaches. Today 85% of Schumacher Group's business processes live inside the public cloud, he says.

The company uses cloud services from providers such as Eloqua for e-mail marketing; Google Apps for e-mail and calendaring; Salesforce.com for CRM software; Skillsoft for learning management systems; and Workday, for human resources management software. "The list continues to go on for us," he says.

Yet Menefee says he doesn't consider himself a cloud advocate. Rather, he says he's simply open to the idea of cloud services and willing to do the cost-benefit and risk analysis.

To be sure, the heavy reliance on cloud services hasn't come without a security rethink, Menefee says. For one, the company needed to revamp its identity management processes. "We needed to think about how to navigate identity management and security between one application and another living out in the cloud," he says.

Indeed, rethinking identity management often is the starting point for enterprises assessing cloud security, says IDC analyst Charles Kolodgy. They have to consider authentication, administrative controls, where the data resides and who might have access to it, for example.

"These are similar to what enterprises do now, of course, but the difference that it no longer owns the infrastructure and doesn't have complete access to the back end so it needs strong assurances," Kolodgy adds.

Start-ups ServiceMesh and Symplified have addressed the need for strong cloud security assurances. ServiceMesh offers Agility Access for use with its Agility Platform, which comprises cloud management, governance and security tools under the platform.

Symplified offers Trust Cloud. Built on the Amazon Elastic Compute Cloud (EC2), Trust Cloud is a unified access management and federation platform that integrates and secures software and infrastructure cloud services, EC2 and Web 2.0 applications.

Schumacher Group uses the Trust Cloud predecessor, Symplified's SinglePoint, an identity, access management and federation service that gives users single sign-on access to multiple cloud applications. SinglePoint also lets IT rapidly provision and de-provision access to all applications in one pass.

Beyond technology, the cloud services model gives rise to a new way of thinking about Schumacher Group's operational resources, Menefee adds.

"Large cloud providers have teams and departments tasked full time, 24/7, to do nothing but protect their customers' sensitive

TIM MUELLER

information and to find continuous improvements to their security, monitoring, intrusion control and so on. As a midsized organization, I don't have a full-time, multiperson department focused entirely on security. With cloud service providers I feel more secure because I get the same benefit as what a Fortune 500 or 100 company would get with a multitenant, secure environment," he says. And, should a security breach occur, "Those teams will be more equipped to do a rapid response than my internal people would."

Certainly with your enterprise data at stake, pushing cloud providers to deliver the security you need is perfectly reasonable. As Forrester Research analyst Chenxi Wang says, "Don't ever compromise any security goals or requirements just because you're moving to the cloud."

Cloud services providers should go the extra mile on security provisioning — and enterprises have to hold them to it contractually, Wang says. "If a cloud services provider says what you want isn't achievable or that it can't provide evidence, you say, 'Look, we'll go to another cloud provider or not to the cloud at all,'" she adds.

Schwan Food, in Marshall, Minn., used that tactic when planning a virtual disaster recovery architecture, says Cory Miller, senior IT operations manager for the multibillion dollar frozen food company.

"We told our providers, 'You are going to use our tools and we are going to extend them into your environment,'" he says. "And I'll do more of that as I expand more into the cloud."

The choice is simple, really. Force providers to work with what you have or find yourself working with yet another set of security tools and interfaces. Chances are, you can even get your security tool vendor to contract with the provider, Miller says.

Along those lines, Reflex Systems, whose virtual firewall Schwan uses to secure its virtualized infrastructure, works with Computer Sciences Corp. and Savvis. The goal is "bringing some consistency to security and management when moving between private clouds and public clouds," the company says.

Schwan fielded solicitations from a number of cloud providers. However, when it came right down to it, not all cloud providers were receptive to Schwan's mandates.

"With several we turned around and said, 'We'll do this and if you're not interested in providing that capability or service to us, we'll go somewhere else and find someone who is,'" Miller says. However, he cautions, "we're considered very mature in our environment ... and I'm not sure smaller companies would have that luxury."

But even small companies would be wise to look out to the future. If you're building a private cloud today with the thought of extending to the public cloud, then knowing what security tools your potential provider will or won't support could impact the technology choices you make, Miller adds.

"You don't want to have designed your private cloud and then find out that the external cloud has such different change management or encryption processes, for example, that it almost offsets the advantages you have in expanding or moving out into the cloud."

Getting tough on cloud providers

As cloud services mature, vendors are working on tools and services to help — if not outright encourage — enterprises to make these sorts of tough demands.

One such tool is Adaptivity's Blueprint4IT. With it, an enterprise can create an IT security blueprint that takes into account factors such as access policies and the sensitivity of data while in transit and at rest, as well as the hardware and software components needed to keep data flowing securely from the internal network into the cloud.

"Take your requirements, generate a blueprint, and hand it to your service providers and say, 'Here's exactly how we'll be setting up our infrastructure and how you're going to guarantee it on the other side as part of our contract,'" says Tony Bishop, founder and CEO of Adaptivity. "Just like you'd hand a blueprint to a general contractor and say, 'Here it is. Go build my house.'"

Or, he adds, enterprises could use Blueprint4IT to assess their service providers and help them score the maturity of their security architectures.

This desire of enterprise customers to conduct their own assessments of a provider's security architecture is something new, agrees Neil Ashizawa, senior manager of HP software-as-a-service products and cloud solutions. Such requests aren't widespread right now, he adds, but HP does field them from time to time and expects to see the numbers grow.

Toward that end, HP offers Cloud Assure, which allows enterprises to scan and do automated penetration testing of networks, operating systems, middleware layers and Web applications for vulnerabilities. This allows the enterprise to get assurance that the cloud provider of choice will be able to carry application workloads securely and keep them safe from unauthorized access, Ashizawa says.

As enterprises approach the public cloud, what they have to remember is that "not every application is going to make sense to be done securely in the cloud, but neither is it that the cloud can't be made secure enough for anything," says Gartner's John Pescatore.

Even financial firms, government agencies or other companies with highly sensitive data such as payment card information or medical records can find the necessary protections in the cloud if they look hard enough, Pescatore says. "I may say, 'That type of data can never go in the cloud' or I might say, 'How about if I find a way to encrypt the data and store it in the cloud?'"

As an example, he cites a demonstration conducted late last year in which the Navy successfully showed it could use a commercial cloud infrastructure-as-a-service platform — in this case Amazon's EC2 — to support its requirements securely. The demonstration included the use of Unisys' ultra-secure access control and security technology, called Stealth.

Developed for U.S. Department of Defense war fighters, the Stealth technology provides data protection for Unisys Secure Cloud services.

When a cloud user logs in and authenticates to the access control mechanism, Stealth figures out who the user is and to which community of interest he belongs and with what security levels. From there, the user only has physical access to participating systems with those security levels. Before a packet traverses the server or storage network, Stealth uses a patented technology to break it into bits, which are then shuffled into three or four "piles." Stealth encrypts each pile separately and then sends them over an encrypted link. The process is reversed at the other end of the connection, Noel says.

Another approach, Pescatore says, is to use dummy data in place of sensitive information out in the cloud. "Applications work fine but sensitive data like payment card information or personally identifiable information stays local," he describes.

Start-up PerspecSys offers this type of functionality, initially for use with the Salesforce.com CRM cloud.

Clearly enterprises have much to think about as they consider using public cloud services. They've got to take a risk-based approach, as has Schumacher Group, with a strong focus on the data and what controls are needed. ■

Hungry for server security

How Schwan Foods satisfied its craving for virtualization-layer security

~ BY BETH SCHULTZ ~

When it comes to sampling innovative technology, Schwan Foods, a multibillion-dollar frozen food producer, digs right in.

The Marshall, Minn., company became an early adopter of VMware ESX Server technology, beginning beta tests in 2001 and launching its formal virtualization project in 2002.

By 2008, Schwan had virtualized two-thirds of its servers, says Cory Miller, the company's senior IT operations manager.

Schwan's virtual server infrastructure today comprises 55 ESX hosts running between 700 and 800 virtual machines (VM). In addition, 44% of the company's 18,000 desktops are virtual, Miller says.

No wonder Schwan began hankering for virtualization-layer security years ago.

When Schwan began its virtualization implementation, it decided to run VMware's ESX on bare-metal hardware.

That was a way to avoid having to worry about operating system patches or security flaws affecting the hypervisor, Miller says. "Still, initially, we used our virtualization for a lot of transactional data but not for credit-card processing or other sensitive data," he adds.

By 2005, Schwan felt comfortable moving sensitive data into the virtual environment. It used traditional physical firewalls to mask, protect and segregate user environments across the development, staging, quality assurance and production networks.

But it didn't take long before problems appeared.

"I could put different kinds of sensitive data — credit card or HIPAA, say — on the same systems and lock them down because we followed the same processes, auditing and compliance for them. But I didn't want to put a SharePoint server on the same host that was processing credit cards," he says. "I could track the data going host to host, but I didn't have the control, monitoring or capabilities to see what was going on within a host."

CORY MILLER, SENIOR IT OPERATIONS MANAGER, SCHWAN FOODS

Addressing that situation meant carving hosts out of the resource pool and creating lockbox environments for sensitive data. And that, in turn, meant Schwan wasn't getting enough throughput or efficiency.

So Schwan immediately began looking for a virtual firewall that could sit at the virtualization layer and do the segregation. It selected vTrust Security from Reflex System, at the time one of the only companies offering a virtual firewall, Miller says.

Schwan can still segment sensitive environments, but now Miller does so out of the entire host pool rather than carving off sections of it, he explains. The virtual firewall inspects traffic on a host and blocks its movement from one guest machine to another.

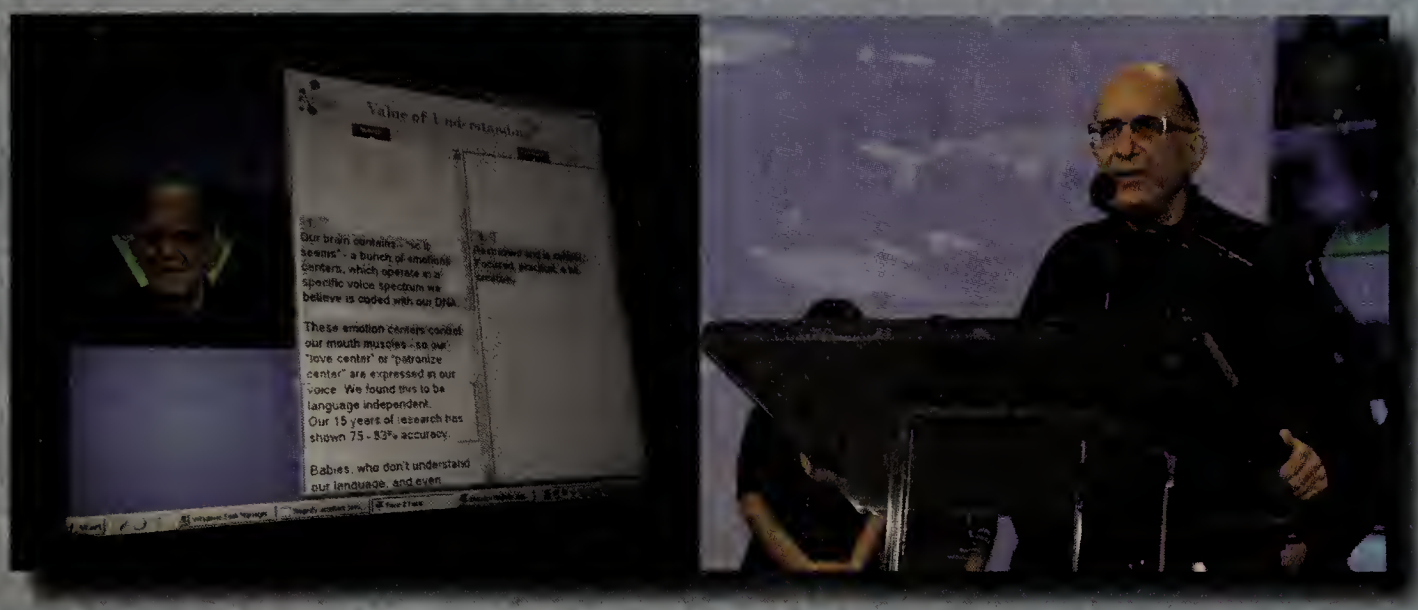
This gives Schwan the ability to run virtual desktops with greater peace of mind, for example. "We might have some executive or high-risk virtual desktops that we keep track of through user monitoring or auditing. We don't want a plant user on the other side of the world being able to get to that person's desktop. Now those virtual desktops can sit on the same hosts and I don't have to worry about the potential for interaction," Miller says.

In its implementation, Schwan was careful to create the same types of firewall rules as it has for the physical firewalls and personal firewalls running on user desktops, Miller says. "That way, guests running on a host are protected within the host and as soon as they exit the virtual switch because they'll move directly into the segmentation created by the physical firewall using the same rule sets," he explains.

This also facilitates auditing. As VMs are moved from host to host through VMware's VMotion technology, they get dropped into the same type of firewall environment or segregated subnet as needed. "By taking a virtual firewall and being able to release those rules so they go across the entire set of hosts within that pool," Miller says, "I'm protected wherever that guest goes."

GREG LATZA

DEMO people's choice



Congratulations to

eXaudios MagInify Call Center

Winner of the DEMO $1 Million People's Choice Media Prize

eXaudios developed capabilities to understand people's emotions through their voice in real time as they speak. Launching at DEMO, this revolutionary new product is designed for call centers and can mitigate escalations, identify fraudulent situations, provide "how-to" recommendations, and monitor performance by management.

Watch their award-winning product launch at:

www.demo.com/DEMOSpring2010PC

www.exaudios.com

eXaudios Technologies

DEMO **Up Next: DEMO Fall, 2010** – September 13-15, Hyatt Regency Silicon Valley. For complete information and to register, go to **www.demo.com**

Participating media prize companies are: CIO COMPUTERWORLD CSO DEMO InfoWorld Macworld NETWORKWORLD PCWorld

Extreme firewall makeover

Skybox, RedSeal lead the way among five vendors with tools to improve firewall efficiency, identify vulnerabilities, meet audit goals.

~ BY ROB SMITHERS ~

Anyone running multiple firewalls in a complex, enterprise environment knows how difficult it can be to catch misconfigurations, avoid conflicting rules, identify vulnerabilities, and meet auditing and compliance mandates.

We looked at five firewall operations management products: AlgoSec's Firewall Analyzer, RedSeal's Network Advisor and Vulnerability Advisor, Secure Passage's FireMon, Skybox's View Assure and View Secure and Tufin's SecureTrack. These products perform similar core functions: they retrieve configuration files of firewalls (and other network devices), store the data and analyze it. They can look at change history, analyze existing rules, perform rules-based queries, re-order rules, and send out alerts, if policies are violated. They can also create automated compliance audit analysis and reports.

They can also do modeling and war-game analysis based on a snapshot-in-time version of the network. Plus, AlgoSec, RedSeal and Skybox can provide network diagrams and topology views of the underlying networks.

Overall, we were most impressed with RedSeal and Skybox, which cover all the basics, plus have the added benefits of being able to support multiple vendor vulnerability scanning products. However, we were impressed with all of the products.

AlgoSec's Firewall Analyzer had an intuitive interface and came with predefined standard audit and analysis reports. Installation was simple and the program offered a wizard for easy data collection.

Network Advisor and Vulnerability Advisor from RedSeal answered questions on how well the network is configured to protect from Internet threats. The programs generate vulnerability reports showing weaknesses in the network, and contain pre-configured compliance management reports.

FireMon from Secure Passage performs real-time analysis on device configuration and stays current by using an automated analysis of compliance guidelines. There is a wizard to import device information en mass for large networks.

Skybox View Assure and Skybox View Secure can automate the collection schedule of configuration files by the hour, day, week, month or year. A built-in ticketing system supports access change tickets and policy violation tickets.

SecureTrack from Tufin has a What-If analysis feature to test changes to policies before they are implemented. Predefined analysis and reporting options are based on industry best practices.

AlgoSec Firewall Analyzer

We tested AlgoSec's Linux-based Firewall Analyzer software package, which consists of an analysis engine, collection engine, Web server, administrative GUI for local and remote administration, and user, policy storage and syslog databases.

The analyzer engine runs queries on the data collected, based on predefined or custom rules, and then generates a detailed report. The Web server sends e-mail alerts to the firewall manager.

We installed it as a VMware appliance on our Dell 600SC server. Once the VMware player is loaded onto the Firewall Analyzer, it boots up, and logging in as root will bring up the Firewall Analyzer browser application.

There are three methods for data collection — a wizard, semi-automated scripts, or doing it manually, which is time consuming and could result in errors.

Once files are retrieved and stored, Firewall Analyzer runs a risk analysis based on PCI compliance, NIST, SANS Top 20 and vendor best practices. In addition, we found that we could create custom analysis reports. Selecting the Firewall Reports option displays charts and a connectivity diagram summarizing changes, findings, policy optimization, rule reordering, firewall information and a firewall connectivity diagram. Choosing the Risks option displays the findings with risk codes and details about the risk with suggestions and diagrams on how to deal with it.

AlgoSec's Change History Report detailed changes in rules on the firewall. On the bottom of the Change History dashboard are features to run interactive traffic queries to compare the report with others, and to create a group report with other firewalls.

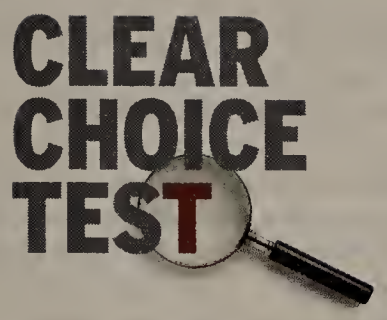
The Optimization Policy feature provides the Rules Cleanup and Reordering tools. Some rule types flagged in a Cleanup Report are labeled as unused, covered, redundant, disabled, and rules with a non-compliant name. The Rule Reordering Report gave us information on how to improve a rule.

The AlgoSec Firewall Analyzer client application dashboard is well organized and multi-tiered, making it easy to find features and wizards. There are pre-defined compliance audits such as PCI-DSS, ISO/IEC27001, Sarbanes-Oxley and others. A drawback was the lack of integration with a vulnerability scanner, but AlgoSec is an excellent product for compliance auditing and compliance and rule optimization.

RedSeal Network Advisor and Vulnerability Advisor

With RedSeal Network Advisor 4.1 and Vulnerability Advisor 4.1, you can automate the process of analyzing, identifying, quantifying and mitigating risk and vulnerabilities in complex networks. Network Advisor uses plugins to import configuration files from each supported device. We could create a unified network topology map with a best practices analysis and solutions for remediation after we imported risk and vulnerability analyses.

Both Network Advisor and Vulnerability Advisor require importing router, switch and firewall configuration files to the database. The analytical engine processes information



that includes host names, IP addresses, subnet masks and device interfaces. Analysis results appear in the form of graphical displays, reports, maps and charts detailing the current status and configuration of the network. Plugins are available for a wide range of products from Cisco, Check Point, Juniper and dozens of others.

After device configuration files are imported into the RedSeal Advisor, the files were checked against RedSeal's best practices database. We could drill down to locate the offending policy by double-clicking on a selected row. Any changes to hosts and devices could be analyzed and reported with the View Changes application.

We accomplished rule usage analysis and reordering by using RedSeal's Custom Best Practice Check feature. Using a regular expression tool, we could search the configuration files and use the available plugin associated with the device. We performed what-if analysis to determine if changes to a rule would adversely affect the network.

RedSeal provides preconfigured compliance management analysis reports. We could add and schedule custom reports to run at specific times. We could analyze and report on how well our network was configured compared to best practice checks, and what assets were exposed to the Internet.

RedSeal's interface for running vulnerability analysis presents a topology map of the network, offering a graphical method for analyzing network vulnerabilities. The map states highly detailed information quantifying the risk, based on the Common Vulnerability Scoring System (CVSS).

RedSeal integrates their product with several well known vulnerability scanners, such as Qualys, nCircle and McAfee. We recommend this product for quantifying risk and vulnerabilities and to allocate resources based on asset value.

FireMon from Secure Passage

FireMon from Secure Passage manages firewalls by reporting on changes to the firewall policy, checking unused rules and reporting how traffic flows through rules. Compliance is safe guarded by the program's automated analysis of compliance guidelines such as PCI and National Security Agency (NSA).

The FireMon architecture includes an application server, data collector and a graphical user interface (GUI). The application server tracked the data collected, performed real-time analysis on transactions and device configuration and generated scheduled reports. The data collector is a FireMon application running on an appliance or PC to monitor and collect data from firewalls, switches and routers.

After installing the FireMon management client on Windows Vista, which was a quick process, we logged into the FireMon server with a user name, password, IP address and port number to bring up the management console.

FireMon offers a wizard for importing Check Point, Cisco, F5, Juniper, Nokia and McAfee/Secure Computing devices. Once the entries are made to the wizard, all the associated firewalls, management servers and log servers are auto-discovered and added automatically in sequence.

We used the Firewall Traffic Flow Analysis tool to produce a report that zeros in on "Any" rules configured on firewalls in a large network. We could fine tune the firewall rules by reducing or eliminating overly permissive "Any" rules and large complicated ones.

We generated FireMon's Rule Recommendation Report that offers analyzing issues, such as a request for https traffic from source and destination addresses. The report showed if a policy existed for the requested access.

We examined the Rule Comparison feature that analyzes the changes to a device's policy rule changes made over time. We saw color-coded icons for change, inserted, deleted and the same. You can revert back to a known good state using this report, which helps with

NETRESULTS

Product	Firewall Analyzer	Network Advisor & Vulnerability Advisor	FireMon	View Assure & View Secure	SecureTrack
Company	Algo Sec	RedSeal	Secure Passage	Skybox	Tufin
Price	$19,900 for FireFlow software $4,995 for appliance $1,900 per firewall $550 audit license	$30,000 base price and $800 per Layer 3 Device for Network Advisor • $30,000 base price and $900/Layer 3 Device for Network Advisor & Vulnerability Advisor	$1,000 per enterprise firewall, site licensing available. Special pricing available for other or smaller environments.	$50,000 for enterprise solution. Additional license cost and consulting / support may be required.	$20,000 for Tufin Security Suite. $5,300 for Tufin Appliance. $600 for SecureTrack Audit license.
Pros	Intuitive interface; predefined industry standard audit analysis and reports. Semi-automated data collection.	Automated import of config files and update scheduling. Powerful tools for determining risk, vulnerabilities, Supports multiple scanning vendors.	Can run what-if analysis. Clear, integrated workflow and planning tool. Custom extensions available for download and development.	Built-in ticketing system. Excellent tools for risk and vulnerability scoring. Multiple third-party vulnerability scanners supported. Network topology mapping .	Well-designed intuitive interface. Pre-configured analysis and reports based on industry best practices. "What-if" analysis.
Cons	Initial configuration file import is not automated. Scanning tools and risk and vulnerability scoring is not supported.	Workflow application not provided. Risk and vulnerability calculations not clearly documented.	Risk and vulnerability scoring are not supported. Scanning tools are not supported.	Difficulty getting the server to start on the first install on Windows XP SP3. Could not get the Microsoft Vista installer to work.	Configuration of devices and SecureTrack software was difficult. Third-party vulnerability scanning vendors not supported.

institutional knowledge transfer.

Secure Passage has an interface that is well organized with features that are easy to navigate. Some of the analysis and report wizards, such as the Rule Recommendation Report, displayed helpful examples showing how to set parameters.

Although the FireMon Rule Comparison Analysis Report was confusing at first with its color-coded parameters that indicated changes, we feel that FireMon has excellent analysis features for optimizing rules and creating audit trails. This product should be considered a good firewall management solution for the enterprise environment.

Skybox View Assure and Skybox View Secure

The Skybox Risk View platform is comprised of two products: the Skybox Secure 4.5 for risk exposure and security profile analysis, and threat alert management, and Skybox Assure that manages the firewall and performs network compliance auditing. The platform application is scalable and is made of the Skybox View Server, Skybox View Collector, Skybox View Manager and Skybox View Dictionary. The dictionary is the database for definitions and profiles for vulnerabilities, threats, worms and network security policies.

Skybox uses vulnerability scanners and analysis to categorize, quantify and prioritize threats to the network. Using the Skybox Assure software suite, we managed network policy validations, regulatory compliance audits and network device changes. With the automation features provided, we ran audit checks on thousands of firewall rule-bases.

We found that the install documentation for Skybox was excellent. Skybox provides several methods to import device configuration files into the Skybox View database. There are also several ways to automate the configuration collection process. If configuration data is located in a database or file repository, the data can be directly imported into Skybox View. You need additional Skybox View Collectors if you want to directly import configuration files on segmented networks.

We used the Operational Console to create tasks using the New Task wizard and selecting a Task Type. There is a convenient option for scheduling collection that can be set for a specific hour, or to be run daily, weekly, monthly or yearly. We could also program the Task Wizard to schedule data import from file repositories with configuration files.

We could create task sequences to run the tasks at a scheduled time.

We saw that APIs were also available to facilitate integration with large third party management tools, such as Opsware, to obtain stored configuration files.

Once the configuration files are loaded into Skybox View, the compliance auditor in Skybox View Assure uses its predefined best-practice access policy to analyze the firewall policies. We used the Policy Compliance Report table to view Violated Rules, Access Compliance and Rule Compliance.

We tested the Risk Exposure Analyzer that simulates potential attack and access scenarios. After Skybox Secure builds a virtual map of the security model, a business impact analysis is created for what-if attack scenarios.

Results of the attack are used to calculate the business impact of a security breach in terms of confidentiality, integrity and availability. Skybox Secure can import business-impact rules and regulations to classify assets and determine an accurate risk assessment metric.

We used the Access Analyzer feature in Skybox View Assure to answer questions about network access. It can be used for What-If model test scenarios and for connectivity analysis on live networks.

For tracking changes, we used the Change Tracking option in Skybox View Assure. We saw that you could keep records of network and firewall changes for compliance recordkeeping.

Skybox View Assure offers change control and workflow with a ticketing system. While the Firewall Compliance Auditor supports Access Change tickets, the Network Compliance Auditor supports both Access Change and Policy Violation tickets.

We were impressed with the modeling capabilities of the SkyBox View Firewall Assurance product. We could simultaneously store three models of the network for running comparison analyses. A side-by-side analysis report makes it effortless to see the changes between two versions of the same network model.

Skybox View Risk Exposure Analyzer presents features to organize the network based on business units and assets. We obtained network vulnerability data from second party vulnerability scanners such as Nessus and Qualys. Using attack scenario options, we generated detailed reports on vulnerabilities uncovered by the simulation. Although we did not see a predefined vulnerability test suite for running attack situations, the Risk Exposure Analyzer is a valuable asset when combined with the modeling capabilities of View Firewall Assurance. Vulnerabilities could be tested on a network model before deploying any equipment.

Tufin SecureTrack

With SecureTrack from Tufin, you can manage and audit firewalls, routers and switches, plus access an incorporated view of firewalls and other devices in your network. SecureTrack supplies automated reporting of risk and audit status, monitors firewall operating systems and supports security compliance standards.

We secured SecureTrack on a VMware appliance. Installation was quick, with no problem. After we saved the settings, the login screen appeared and we could access the Tufin SecureTrack server.

The screen has icons for Policy Change Reports, Rule Usage Statistics, Security Risk Reports and Best Practices Audit. Users can choose to be notified immediately of policy changes and to receive weekly reports.

Optimization and cleanup is a big part of SecureTrack's capabilities. With the goal of ensuring the rule base is not in violation of corporate and regulatory compliance, SecureTrack continually monitors firewalls, routers and switches. The SecureTrack Compare feature lists the number of recent revisions next to the device name. New revision alerts appear when revisions are generated. The Revision List can be filtered based on 10 attributes.

We used SecureTrack Analyzer to identify overlapping and redundant rules. To access predefined best practice policies that are stored in the SecureTrack database, we used the Audit and Compliance option. There are best practice checks for all firewalls and specific firewalls such as Check Point. SecureTrack also offers predefined policy analysis audits for PCI-DSS compliance. You can also set up alerts to be sent when security policy rule changes are made.

We found the browser dashboard to be crisp and well laid out. We liked the Compare Analysis option for comparing firewall revisions and maintaining the audit trail.

Custom firewall audits were created with the SecureTrack Audit wizard for detailed answers on compliance policies. An impressive list of predefined audit templates can be selected with a wizard, thereby saving time. There is also a predefined PCI-DSS audit analysis feature used to create reports for audit policy with a summary detailing the compliance verification.

We liked the Security Trend analysis reports with charts, graphs and a summary table displaying risk scoring. Tufin does not base the scores on the CVSS as is common practice with similar products. We did find SecureTrack to be a good product for auditing and maintaining compliance with best practices based on industry and corporate policies. ■

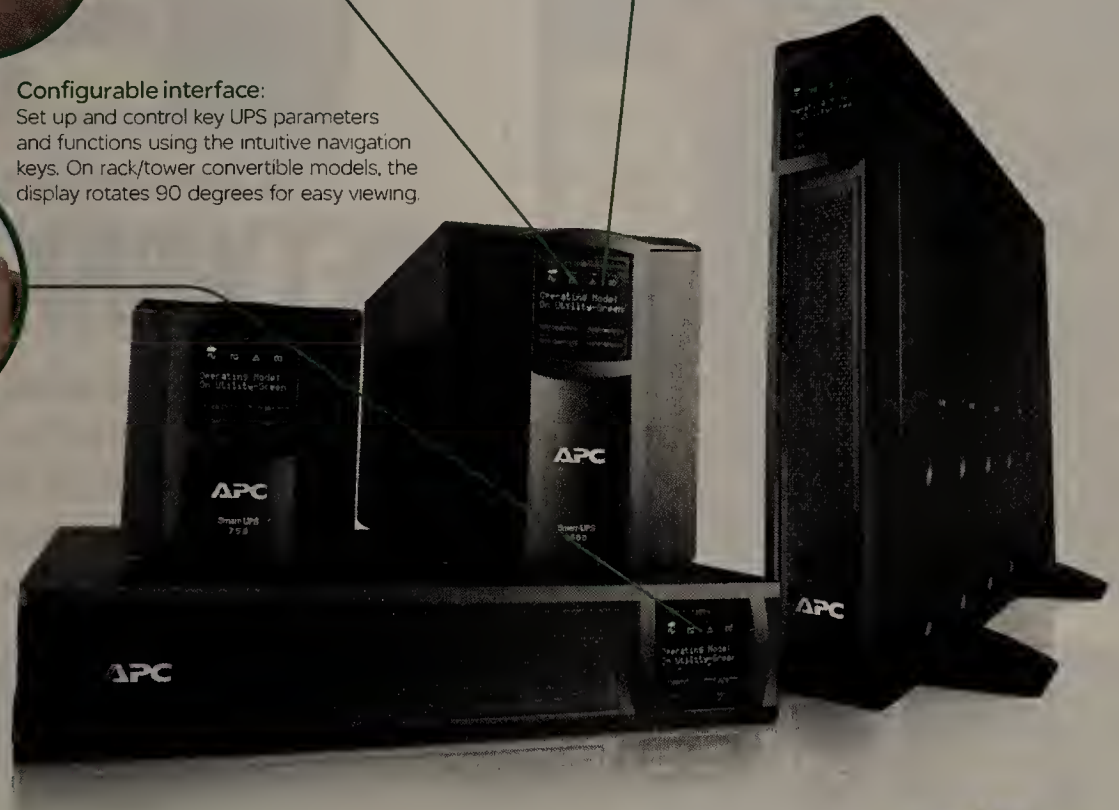
Smithers is a Network World Test Alliance Partner and CEO of Miercom, a testing lab and network consultancy. He can be reached at rsmithers@miercom.com.

Announcing the new, interactive energy-saving Smart-UPS from APC.

Intuitive alphanumeric display:
Get detailed UPS and power quality information at a glance – including status, about, and diagnostic log menus in your choice of up to five languages.

Energy savings:
A patent-pending "green" mode achieves online efficiencies approaching 99 percent, reducing heat loss and utility costs.

Configurable interface:
Set up and control key UPS parameters and functions using the intuitive navigation keys. On rack/tower convertible models, the display rotates 90 degrees for easy viewing.



If you want Legendary Reliability™ inside, it had better say APC™ outside.

What do you get when you combine 25 years of Legendary Reliability with the latest in UPS technology? Introducing the new APC Smart-UPS™ range of interactive, intuitive, and energy-saving UPSs, designed to protect critical server and network equipment from power threats and downtime.

New APC Smart-UPS: Smarter. Easier. Greener.

Thanks to millions of dollars in research, APC can proudly claim that only the new Smart-UPS features the unique battery life expectancy predictor, telling you the exact month and year for battery replacement. Precision temperature-compensated charging extends battery life; unique power meter function monitors energy usage; and a patent-pending "green" mode boosts online efficiencies up to 99 percent, saving on utility costs. Plus, the interactive LCD provides detailed status, configuration, and diagnostic information previously available only via software.

When dollars count and performance is critical, insist on the more intelligent, more intuitive APC Smart-UPS. Now more than ever, the name on the outside guarantees reliability on the inside: APC Smart-UPS.

APC Legendary Reliability®

Only APC offers the most technologically advanced, user-friendly features, and the guaranteed reliability you need to protect your critical data and equipment. Look for APC on the outside to ensure Legendary Reliability on the inside.

Download a FREE copy of APC White Paper #10, "Preventing Data Corruption in the Event of an Extended Power Outage."

Visit www.apc.com/promo Key Code t460w
Call 888-289-APCC x6198 • Fax 401-788-2797

APC™ by Schneider Electric

NETWORKWORLD

Editorial Index

Advertiser Index

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

International Data Group
CHAIRMAN OF THE BOARD: Patrick J. McGovern

IDG Communications, Inc.
CEO: Bob Carrigan

Network World is a publication of IDG, the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 300 computer publications in 85 countries. One hundred million people read one or more IDG publications each month. Network World contributes to the IDG News Service, offering the latest on domestic and international computer news.

Publicize your press coverage in Network World by ordering reprints of your editorial mentions. Reprints make great marketing materials and are available in quantities of 500 and up. To order, contact the YGS Group, (800) 290-5460 ext. 148 or e-mail networkworld@theygsgroup.com.

Network World Events and Executive Forums produces events including IT Roadmap, DEMO and The Security Standard. For complete information on our current event offerings, call us at 800-643-4668 or go to www.networkworld.com/events.

Periodical postage paid at Framingham, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #PM40063731. Network World (ISSN 0887-7661) is published twice monthly by Network World, Inc., 492 Old Connecticut Path, Framingham, MA 01701-9002. **Network World** is distributed free of charge in the U.S. to qualified management or professionals. To apply for a free subscription, go to www.subscribenw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-877-701-2228. Non-qualified subscribers: $5.00 a copy; U.S.—$129 a year; Canada—$160.50 (including 7% GST, GST#126659952); Central & South America—$150 a year (surface mail); all other countries—$300 a year (airmail service). Digital annual subscription rate of $29.99. Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication. Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zebb Road, Ann Arbor, Mich. 48106. **PHOTOCOPYRIGHTS:** Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by Network World, Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3.00 per copy of the article, plus 50 cents per page is paid to Copyright Clearance Center, 27 Congress Street, Salem, Mass. 01970. **POSTMASTER:** Send Change of Address to Network World, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9.

USPS735-730

Network World, Inc.

492 Old Connecticut Path,
Framingham, MA 01701-9002
Phone: (508) 766-5301

To Send E-Mail to NWW Staff
firstname_lastname@nww.com

CEO: Mike Friedenberg
SVP, CHIEF CONTENT OFFICER: John Gallant
SVP, GROUP PUBLISHER: Bob Melk
PUBLISHER: Andrea D'Amato

Online Services
SVP, GM ONLINE OPERATIONS: Gregg Pinsky
DIRECTOR ONLINE SERVICES: Elisa Della Rocco
MANAGER, ONLINE ACCOUNT SERVICES: Danielle Tetreault

Custom Solutions
SVP STRATEGIC PROGRAMS & CUSTOM SOLUTIONS GROUPS: Charles Lee

Events
SVP, EVENTS: Ellen Daly
VP, EVENT MARKETING: Mike Garity
DIRECTOR OF EVENT OPERATIONS: Deb Begreen

Marketing
VP MARKETING: Sue Yanovitch

Ad Operations
SENIOR PRODUCTION MANAGER: Jami Thompson
ADVERTISING COORDINATOR: Maro Eremyan

Finance
VP FINANCE: Mary Fanning

Human Resources
SVP HUMAN RESOURCES: Patricia Chisholm

Circulation/Subscription
CIRCULATION MANAGER: Diana Turco, (508) 820-8167

IDG List Rental Services
DIRECTOR OF LIST MANAGEMENT: Steve Tozeski
TOLL FREE: (800) IDG-LIST (US only)/Direct: (508) 370-0822

Sales

Northeast/Midwest/Central
REGIONAL ACCOUNT DIRECTOR: Timothy Keough, (508)766-5475

Southeast/Mid-Atlantic
REGIONAL ACCOUNT DIRECTOR: Jacqui DiBianca, (610) 971-0808, FAX: (201) 621-5095

Northern California/Northwest
REGIONAL ACCOUNT DIRECTOR: Jessica Koch, (415)267-4522

Silicon Valley/Southwest/Rockies/Utah
REGIONAL ACCOUNT DIRECTOR: Coretta Wright, (415) 267-4515

Marketplace/Emerging Markets–National
REGIONAL ACCOUNT MANAGER: Enku Gubaie, (508) 766-5487

ONLINE

Northeast/Midwest/Central
ONLINE ACCOUNT DIRECTOR: Debbie Lovell, (508)766-5491

East
REGIONAL ACCOUNT DIRECTOR: Jacqui DiBianca, (610)971-0808

Northern California/Northwest/Rockies/Utah:
ONLINE DISTRICT MANAGER: Katie Layng, (415) 267-4518

Northern California/Southwest
ONLINE REGIONAL ACCOUNT MANAGER: Katie Albang, (415) 267-4510

Custom Solutions
EASTERN SALES DIRECTOR: Tom Grimshaw, (508) 988-6941
WESTERN SALES DIRECTOR: Karen Wilde, (415) 267-4512

Event Sales

DEMO
SVP, NETWORK WORLD EVENTS & DEMO: Neal Silverman, (508) 766-5463

IT Roadmap
REGIONAL ACCOUNT DIRECTOR, WESTERN REGION: Jennifer Sand, (415) 267-4513
REGIONAL ACCOUNT DIRECTOR, EASTERN REGION: Michael McGoldrick, (508) 766-5459

BACKSPIN | BY MARK GIBBS

Waiting for change

EVERYTHING CHANGES if you wait long enough. For example, did you know that the Internet is finished? Yep, the artist formerly known as Prince (who now seems to be known as Prince again) declared a few days ago that "The Internet's completely over ... The Internet's like MTV. At one time MTV was hip and suddenly it became outdated." Thanks Prince, good to know.

Anyway, here in Ventura, Calif., we're waiting for the weather to change. Sure, we normally have "June gloom" but this is usually followed by glorious, sunny weather that is, dare I say it, exquisite. However this year, April was sort of gloomy, May was mostly gloomy, June was gloomier than usual, and now July is trying to out-do June. This is ridiculous. You pay heavily to live in California, but usually with such great weather you feel like there's a reason for the expense. This year, we all deserve a tax refund.

And talking about things that are changing, or, at least, reputedly changing, I have to revisit my recent rant about Sprint's customer service, or rather lack thereof.

In that column I addressed my criticisms to Sprint's CEO, Dan Hesse, pointing out that Sprint doesn't care about existing customers. Its pricing for a replacement phone one year into a two-year contract was ridiculous given I could pay the early termination fee and go to another service provider and get a better phone for a lot less money.

As I discussed a couple of weeks ago, I switched, of all things, to a Sprint service reseller, Credo, and am quite happy and much better off. Then about a week after my switch, a press release from Sprint landed on my virtual doorstep.

The release said, with an air of smug self-satisfaction, that Sprint is changing: "It's one thing to grow a company ground-up on a commitment to deliver an outstanding customer experience [could that be a jibe at the likes of Credo?]. It's quite a different feat to introduce the concept to a multi-billion dollar enterprise."

It continued: "Sprint is changing its tune — externally and internally — to hold onto customers in an industry with one of the highest churn rates. Sprint ... has flipped its strategy to focus on a singular mission: improve the customer experience. "

Oh, really? I ask because as I wrote in my previous column, I saw no evidence of this new, improved "tune" when I was talking to Sprint customer service; all I heard was the same old, tired dirge that scores of readers of this column have written in about. That dirge has, as a backing track, the industry standard business-as-usual hum of disinterest in the customer.

The Sprint press release added, "Gartner will announce Sprint as the winner of its CRM Excellence Award in the 'Customer Experience' category," from which I conclude that all cell phone service providers stink (which, according to you, dear readers, is the case). Sprint must therefore stink least.

In spite of my snarky disbelief I'm going to give Sprint the benefit of the doubt here and hope it can live up to its press release hyperbole because change is always possible. That said, I'm betting that unlike waiting for better weather here in Ventura, major improvement in Sprint's customer service could be much longer coming. ■

Reach Gibbs in Ventura, Calif. at backspin@gibbs.com.

NETBUZZ | BY PAUL MCNAMARA

Taking distracted driving to the next level

HEADED WEST on the Massachusetts Turnpike, I pass a car being operated by a young woman who has both hands firmly on the steering wheel, just like they teach when you get your license. Rather than the classic 10 o'clock and 2 o'clock positioning, however, hers are clamped more like 11:45 and 12:15, or the optimum setup for thumb-texting on whatever mobile device it was she had balanced in between... And texting she was, most furiously.

Dangerous behavior, yes, but barely noteworthy these days and not what made me do the triple-take.

What did? That would be her left foot. Her left foot?

You heard me, her left foot, which instead of being on the floorboard near its significant other, her right foot, was sticking out the driver's side window practically begging passersby to play This Little Piggy. ("This little piggy went to market ... this little piggy is admiring itself in the side-view mirror ...")

Texting like a madwoman, toes flapping in the breeze, tooling on down the highway: This diva was not only the embodiment of distracted driving, but a genuine trailblazer.

Coincidentally, Massachusetts on July 2 became the 29th state to outlaw texting while driving, although clearly the prohibition had failed to impress Miss Twinkle-Toes, presuming someone had bothered to message her the news. And my guess would be that she didn't notice my head shaking as I passed her either.

At least she wasn't speeding.

(Final thought: Yes, it has occurred to me that I didn't see what I think I saw; that this scene was actually a variation of the old foot-sticking-out-of-the-trunk gag. Maybe. But the young lady and her seat were definitely reclined, as if to facilitate a full-scale left-foot escape; so if it was a gag it was a darn good one.)

Wikipedia's million-dollar faux pas

Hey, look, someone donated a million dollars to Wikipedia — anonymously, no less.

At least that was the headline on Digg and we could all see it was true because there was a link to the database of donors and a screen capture with a red circle around the amount and everything.

A million smackaroos from a benefactor too shy to accept a public thank-you? Now that's news, so I fired off an e-mail to Jay Walsh, Wikipedia's head of communication, to see if it was indeed true and if he could tell me anything at all about the bashful donor. Walsh's reply:

"In fact it turns out there was a slight glitch in how that donation was reported through our system. The amount is 100% correct, but the donation should have been attributed to the Alfred P. Sloan Foundation. We've corrected the link. This is the third part of a three-year, one million dollars per year grant that was announced back in March, 2008.

"Glad the Digg folks pointed this out, and we're now tracking the comment/donation input system a bit more carefully."

There are easy wisecracks to be made here about Wikipedia and accuracy. Too easy. ■

Of course, rarely does a week go by without someone helpfully drawing attention to an error of my own doing. The address is buzz@nww.com.

Cross-country network.
Cross-town support.

Introducing CenturyLink™ Business

CenturyTel and EMBARQ have merged—and the result is CenturyLink, delivering top-tier business data network solutions to customers throughout the U.S. You can count on us to combine a state-of-the-art national network with local support from people right in your own community.

Partner with CenturyLink and make sure your business is Stronger Connected™—across country and across town.

Learn more at centurylink.com/stronger or call 1-866-345-0814.

CenturyLink™ Business
Stronger Connected™

CHANGE

the rules of networking.

HP is changing networking.

Gone are the days of networks that are hard to manage, vulnerable to attacks, and expensive to maintain. With HP game-changing solutions, the status quo is history.

The New Rules of Networking

#1 Simplified network designs that are twice as secure[1]

#2 Up to 2x better performance for greater flexibility[2]

#3 Up to 65% lower cost of ownership[3]

Put the new rules to work for you.
hp.com/networking/change

Outcomes that matter.

1. Respondents from Infonetics September 2008 survey report that Tipping Point blocks 2.3x more threats compared to next-closest competitor

2. Based on line rate comparison between HP 12518 128x 10G (2.2 Bpps) and Cisco Nexus 7000 Series 18 (960mpps)

3. IDC white paper sponsored by HP, *ROI of Switched Ethernet Networking Solutions for the Midmarket*, #219843, August 2009